Digitaliserings-
styrelsen

DATATILSYNET

Slutrapport for sandkasseforløb med Børns Vilkår

# Samtalesimulator til træning af svære samtaler med børn

Juni 2026

# Indhold

# Forord

***Den regulatoriske sandkasse er et gratis tilbud til virksomheder og myndigheder, som skal bidrage til at tilvejebringe ansvarlige og lovlige AI-løsninger.***

Den regulatoriske sandkasse for AI ("kunstig intelligens") er et samarbejde mellem Datatilsynet og Digitaliseringsstyrelsen, hvor virksomheder, myndigheder og organisationer kan få gratis adgang til relevant ekspertise og vejledning i forbindelse med et konkret AI-projekt.

Formålet med den regulatoriske sandkasse er at understøtte innovation og ansvarlig brug af AI-løsninger gennem projekt- og praksisnær vejledning om konkrete regulatoriske rammer, og dermed bidrage til at sikre ansvarlig og lovlig anvendelse af AI-løsninger. Gennem denne vejledning er det samtidig målet at bidrage til at nedbringe tiden fra udvikling til drift og reducere risikoen for, at projekter forsinkes eller opgives på grund af usikkerhed om de regulatoriske krav.

Sandkasseforløbene giver Datatilsynet og Digitaliseringsstyrelsen et detaljeret indblik i de regulatoriske udfordringer, som virksomheder, myndigheder og organisationer kan støde på, når de udvikler og anvender innovative AI-løsninger. Erfaringer fra sandkasseforløbene indgår derfor samtidig i myndighedernes generelle vejledningsarbejde med henblik på at bidrage til at sikre ansvarlig og lovlig udvikling samt anvendelse af AI-løsninger.

Den regulatoriske sandkasse blev etableret i efteråret 2023, og den første runde af den regulatoriske sandkasse blev gennemført i 2024. Ansøgningsfristen for deltagelse i den anden runde udløb den 4. april 2025. Sandkassen modtog i alt 18 ansøgninger, hvoraf 4 ansøgninger var fra offentlige myndigheder, 11 ansøgninger var fra private virksomheder og 3 ansøgninger var fra foreninger. Et tilbagevendende tema var brugen af tale-til-tekst-teknologier og anvendelse af generativ AI til at skabe overblik over sager, dokumenter mv. Derudover vedrørte flere ansøgninger udviklingen og anvendelsen af AI-løsninger i sundhedssektoren, der skal optimere patientbehandling og de bagvedliggende arbejdsprocesser. Blandt nogle ansøgninger var der desuden en ambition om at bruge AI til at træne og forbedre fagprofessionelles kompetencer.

Efter en gennemgang af ansøgningerne udvalgte Datatilsynet og Digitaliseringsstyrelsen to AI-projekter. Det ene AI-projekt står Børns Vilkår bag, og det andet står startupvirksomheden BrainCapture ApS (herefter "BrainCapture") bag.

Deltagerne har i vejledningsforløbene i denne runde i den regulatoriske sandkasse modtaget vejledning om konkrete databeskyttelsesretlige problemstillinger. Derudover blev vejledningen udvidet i forhold den første runde, så deltagerne også har modtaget vejledning om risikoklassifikation efter forordningen om kunstig intelligens (herefter "AI-forordningen").

AI-projektet hos Børns Vilkår var under sandkasseforløbet i opstarts-/udviklingsfasen. Der var derfor endnu ikke et fuldstændigt overblik over AI-systemets opbygning, og alle interne processer. AI-projektet udviklede sig derudover også under sandkasseforløbet både i forhold til, hvem der skulle udvikle og bruge AI-løsningen i drift.

Børns Vilkår havde forinden sandkasseforløbets opstart grundigt overvejet, hvordan samtalesimulatoren skulle fungere. Derudover havde Børns Vilkår også gjort sig en række relevante overvejelser i forhold til AI-retlige og databeskyttelsesretlige problemstillinger, der blev taget udgangspunkt i ved tilrettelæggelsen af rammerne for vejledningsforløbet i den regulatoriske sandkasse.

# 1.Sammendrag

## 1.1. Børns Vilkårs samtalesimulator

Børns Vilkår ønsker i første omgang at udvikle en samtalesimulator, der gør brug af AI, og som giver bedre muligheder for fagprofessionelle hos bl.a. kommuner at træne svære samtaler med børn og unge i et simuleret, fiktivt miljø. Løsningen skal fungere som et støtteværktøj. Fordelen herved er, at man kan træne håndteringen af svære samtaler uden at involvere børn og unge i processen. Det er formålet at nedbringe de negative konsekvenser, som kan være forbundet med træning i håndtering af svære samtaler med børn og unge i en faktisk og konkret rådgivningssituation, ligesom at samtalesimulatoren kan fungere som et supplerende værktøj til andet læringsmateriale og undervisning.

AI-løsningen skal bestå af to dele: 1) en menneskelignende AI-dreven video chatbot - der af Børns Vilkår er navngivet "barnebotten" – som skal kunne gennemføre en samtale med f.eks. en børne- og ungerådgiver eller anden fagprofessionel hos Børns Vilkårs kunder (f.eks. kommuner) og 2) en "coachbot", som modtager og analyserer outputtet fra samtalen mellem den fagprofessionelle og barnebotten, og som derefter omsætter det til feedback til den fagprofessionelle. For en uddybende beskrivelse af løsningen henvises der til afsnit 2.

## 1.2. Temaer og væsentlige konklusioner

Datatilsynet og Digitaliseringsstyrelsen har som led i sandkasseforløbet hjulpet Børns Vilkår i forhold til risikoklassificering af AI-løsningen samt med at vurdere en række databeskyttelsesretlige problemstillinger. Det bevirker imidlertid ikke, at AI-løsningen derved er certificeret eller godkendt af Datatilsynet eller Digitaliseringsstyrelsen.

Nedenfor følger en beskrivelse af temaerne og væsentlige konklusioner i Børns Vilkår sandkasseforløb.

- **Personoplysningsbegrebet:** Det første en dataansvarlig bør vurdere ved udvikling eller anvendelse af en AI-løsning er, om det datasæt, der benyttes, indeholder personoplysninger, og dermed falder ind under databeskyttelsesreglernes anvendelsesområde. Det er en afgørende forudsætning for at kunne overholde databeskyttelsesreglerne. Databeskyttelsesreglerne indeholder en bred definition af, hvad der udgør personoplysninger. Det indebærer bl.a., at den dataansvarlige bør være opmærksom på, om oplysninger, som ønskes anvendt rent faktisk er anonymiseret, eller om der er tale om pseudonymiserede oplysninger, der som udgangspunkt anses for at være personoplysninger.

- **Rolle- og ansvarsfordeling:** Det er vigtigt, at Børns Vilkår – eventuelt i samarbejde med deres kunder og IT-leverandør – fastlægger, hvilke databeskyttelsesretlige roller Børns Vilkår har i forbindelse med samtalesimulatoren, idet kravene til dataansvarlige og databehandlere er forskellige. Børns Vilkår har i sandkasseforløbet kortlagt Børns Vilkårs og de øvrige aktørers rolle- og ansvarsfordeling på tværs af de forskellige procestrin i udviklingen og driften af samtalesimulatoren.

- **Retligt grundlag:** Ved Børns Vilkårs egen brug af samtalesimulatoren til kompetenceudvikling af medarbejdere/frivillige rådgivere skal det vurderes, om selve behandlingen af personoplysninger om disse personer er nødvendige af hensyn til Børns Vilkårs opfyldelse af ansættelseskontrakterne med dem, hvis artikel 6, stk. 1, litra b skal anvendes som behandlingsgrundlag.

  I forhold til Børns Vilkårs ønske om at behandle personoplysninger i forbindelse med adgangskontrol og licensstyring, kan det være hensigtsmæssigt at undersøge, om databeskyttelsesforordningens artikel 6, stk. 1, litra c kan anvendes som behandlingsgrundlag.

  Anvendelsen af artikel 6, stk. 1, litra f som behandlingsgrundlag kræver en konkret vurdering af om behandlingen af personoplysninger i forbindelse med de pågældende formål er nødvendig for, at Børns Vilkår kan forfølge en legitim interesse, som ikke overgås af de registreredes grundlæggende interesser og frihedsrettigheder. En sådan vurdering skal i øvrigt dokumenteres.

- **Konsekvensanalyse:** Børns Vilkår skal – i de tilfælde hvor Børns Vilkår er dataansvarlig – foretage en konsekvensanalyse, hvis behandlingsaktiviteten sandsynligvis vil indebære en høj risiko for fysiske personers rettigheder og frihedsrettigheder. Det er i den forbindelse relevant at få klarlagt, om der behandles personoplysninger ved brug af ny teknologi.[1] Det vil efter Datatilsynets opfattelse normalt være tilfældet ved udvikling og brug af AI-løsninger. Derudover er det relevant at få klarlagt, om AI-løsningen i driftsfasen indebærer behandling af særlige kategorier af oplysninger, behandling af oplysninger om sårbare personer eller behandling af personoplysninger i stort omfang.

- **AI-system:** Når Børns Vilkår skal vurdere, om deres løsning er omfattet af AI-forordningen, skal de først og fremmest vurdere, om deres løsning udgør et "AI-system".

  En central læring i denne sammenhæng er, at vurderingen af, om et konkret softwaresystem falder ind under definitionen af et AI-system efter AI-forordningen, ikke alene bør baseres på en isoleret og teknisk opdeling af løsningen i enkeltstående komponenter. Vurderingen bør i stedet baseres på systemets specifikke arkitektur og funktionalitet samt tage hensyn til de syv elementer i definitionen af et AI-system. Børns Vilkårs løsning bør samlet set udgøre et "AI-system" efter AI-forordningen (afsnit 4.2).

- **Undtagelser til AI-forordningen:** I forbindelse med risikoklassificeringen af Børns Vilkårs AI-system, er det relevant at fremhæve, at udviklings- og afprøvningsaktiviteter *inden* AI-systemet er bragt i omsætning, er undtaget kravene i AI-forordningen. Dermed vil Børns Vilkårs AI-system først blive omfattet af AI-forordningen, når det er bragt i omsætning/placeret på markedet (afsnit 4.3).

- **Risikoklassificering af AI-systemet:** Risikoklassificeringen af Børns Vilkårs AI-system afhænger af AI-systemets tilsigtede formål og anvendelse. Børns Vilkår skal have for øje at sikre, at AI-systemet *ikke* anvender biometriske data til at udlede følelsesmæssige tilstande hos ansatte

[1] 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, s. 9.

på en arbejdsplads eller studerende på en uddannelsesinstitution. Sådan brug kan indebære en forbudt AI-praksis (afsnit 4.4.1).

Hvis AI-systemet bruges i uddannelsesregi til at evaluere elevernes præstationer for derved at styre den enkeltes videre læringsproces, kan systemet efter de konkrete omstændigheder udgøre et højrisiko-AI-system. Hvis Børns Vilkårs AI-system implementeres på arbejdspladser, kan det ud fra omstændighederne tilmed udgøre et højrisiko-AI-system. Det afhænger af, om det konkret anvendes til at "overvåge" og "evaluere" ansattes præstationer og adfærd (afsnit 4.4.2).

Børns Vilkårs AI-system er herudover tilsigtet at interagere direkte med brugere af systemet, hvorved dele af AI-forordningens gennemsigtighedsforpligtelser er relevante (afsnit 4.4.3).

- **Børns Vilkårs rolle i AI-værdikæden:** Når Børns Vilkår skal vurdere, hvilken rolle i AI-værdikæden de har i relation til det konkrete AI-system, er det væsentligt at have for øje, at en udbyder af et AI-system ikke selv behøver at udvikle et AI-system for at være udbyder, men derimod godt kan få udviklet og leveret et AI-system. Det afgørende i den forbindelse er, hvor stor en indflydelse Børns Vilkår har på udviklingen og tilpasningen af AI-systemet, samt hvorvidt Børns Vilkår videregiver AI-systemet under eget navn og mærkevare (afsnit 4.5).

## 1.3. Væsentlige overlap mellem databeskyttelsesreglerne og AI-forordningen

AI-forordningen fastlægger en juridisk ramme for udvikling og anvendelse af AI. Reglerne følger en risikobaseret tilgang, hvor graden af forpligtelser følger graden af risici mod sundhed, sikkerhed og de grundlæggende rettigheder, der er forbundet med anvendelsen af AI, dvs. jo højere risiko desto strengere krav. Forordningen indfører bl.a. en række krav til udbydere og idriftsættere af højrisiko-AI-systemer, f.eks. krav om risikostyring, teknisk dokumentation, menneskeligt tilsyn, logning, rapportering af hændelser mv.

Databeskyttelsesreglerne finder anvendelse på al behandling af personoplysninger, der helt eller delvis foretages ved hjælp af automatisk databehandling.[2] Ifølge databeskyttelsesreglerne har enhver ret til beskyttelse af sine personoplysninger, og enhver, der behandler personoplysninger om andre i ikke-privat sammenhæng, er forpligtet til at iagttage disse rettigheder og til at beskytte personoplysningerne.

Da udviklingen og anvendelsen af AI-systemer, herunder højrisiko-AI-systemer, typisk indebærer en behandling af personoplysninger, finder begge regelsæt ofte anvendelse samtidig. AI-forordningen ændrer i den forbindelse ikke ved gyldigheden af databeskyttelsesreglerne.[3] Der er dog flere overlap mellem forpligtelserne. Begge regelsæt stiller f.eks. krav om risikovurdering, dokumentation og ansvarlighed. Databeskyttelsesreglerne kræver bl.a. retligt grundlag, dataminimering, gennemsigtighed og gennemførelse af konsekvensanalyser (DPIA) ved høj risiko, mens AI-forordningen – især for højrisiko-AI – pålægger krav om bl.a. risikostyring, datakvalitet, teknisk dokumentation, menneskeligt tilsyn og løbende overvågning. I praksis vil organisationer således ofte have gavn af at sammentænke deres arbejde med at sikre overholdelse af de to regelsæt, da kravene i et vist omfang supplerer og understøtter hinanden.

[2] Databeskyttelsesforordningens artikel 2, stk. 1.
[3] AI-forordningens præambelbetragtning 10.

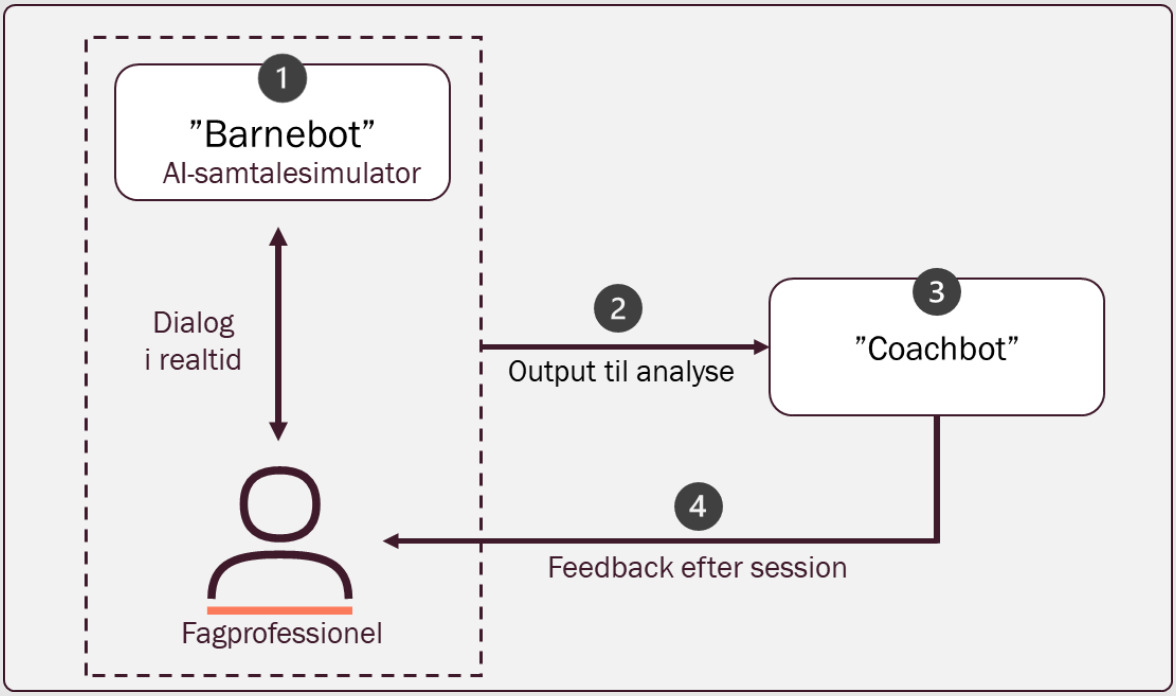
# 2. Projektbeskrivelse

## 2.1. Beskrivelse af Børns Vilkårs samtalesimulator

Børns Vilkår er en social humanitær interesseorganisation, der arbejder for at stoppe svigt af børn og unge i Danmark, hvad enten børnene svigtes af deres nærmeste, myndighederne eller af samfundet. Som en del af dette arbejde har Børns Vilkår startet et projekt med henblik på at udvikle en samtalesimulator, der skal bruges til træning af fagprofessionelle. Samtalesimulatoren vil indgå som en del af et samlet forløb, hvor den fagprofessionelle trænes i Børns Vilkårs principper for samtaler med børn, samt introduceres for relevant lovgivning og andre relevante emner.

Projektet har til formål at give fagprofessionelle bedre mulighed for at træne håndteringen af svære samtaler med børn – uden at skulle involvere faktiske børn. På nuværende tidspunkt har fagprofessionelle (børne- og unge-rådgivere i kommunerne, lærere, socialrådgivere, socialpædagoger osv.) kun mulighed for at "træne" disse samtaler, når de har samtaler med børn, der befinder sig i reelle og ofte sårbare situationer. Konsekvenserne af at gribe en vanskelig samtale med et i forvejen udsat barn uheldigt an, kan have stor negativ indvirkning på børnene og deres videre forløb. Samtalesimulatoren giver således fagpersoner mulighed for at træne samtalerne i et simuleret, fiktivt miljø via interaktion med samtalesimulatoren.

Den samlede løsning ("AI-løsningen") omkring AI-samtalesimulatoren uddybes nedenfor, og kan illustreres på følgende vis:




Figur 1: Illustration af Børns Vilkårs "AI-løsning"

1) **"Barnebot":** Som det første trin i løsningen skal en fagprofessionel gennemføre en samtale med en AI-samtalesimulator, der af Børns Vilkår er navngivet "Barnebotten". AI-samtalesimulatoren skal repræsentere og agere et barn med problemer af forskellig art (via en "avatar"), og skal være i stand til at svare på realistisk vis, som et barn vil gøre, herunder give undvigende svar, agere stille, svare kortfattet osv.
   AI-samtalesimulatoren forventes at bestå af flere forskellige AI-komponenter, der sikrer løsningens samlede funktionalitet, herunder f.eks. komponenter som transskribering, taleforståelse, taleanalyse, udledning af nonverbal kommunikation og svargenerering/talesyntese. AI-samtalesimulatoren baserer sig herudover på en stor sprogmodel (Large Language Model, "LLM").
   På tidspunktet for vejledningsforløbet var der ikke fuld klarhed over datagrundlaget for løsningen.

2) **Output til analyse:** Baseret på samtalen mellem den fagprofessionelle og AI-samtalesimulatoren, genereres et output, som skabes gennem de ovenfor beskrevne komponenter under første trin. Input fra brugeren samt det genererede output fra "barnebotten" sendes videre til "coachbotten" til videre behandling.

3) **"Coachbot":** "Coachbotten" modtager og analyserer outputtet fra samtalen mellem den fagprofessionelle og "barnebotten". "Coachbotten" foretager analysen af samtalen ud fra en række parametre, som Børns Vilkår - baseret på faglig indsigt og erfaring - ved, har betydning for en god samtale med et barn. Dette kunne f.eks. være parametre som inddragelse af barnets perspektiv, evnen til at rammesætte en samtale ud fra Barnets Lov, oplysning omkring rettigheder, aktiv lytning og evnen til at skabe en tryg dialog.

4) **Feedback**: "Coachbottens" analyse omsættes til feedback til den fagprofessionelle om, hvordan samtalen er forløbet. Feedbacken består i vejledning om, hvordan samtalen kan forbedres, hvilket afhænger af den konkrete situation. Dette kunne f.eks. være feedback om, at den fagprofessionelle anvender ord, der kan være svære for et barn at forstå.
   Den feedback, der gives, er generelt målrettet de læringsmål, som er opsat for det konkrete scenarie, og de kan variere betydeligt afhængigt af, hvor i et træningsforløb man befinder sig, og hvilken type fagprofessionel man er. Feedback dannes ud fra mange komponenter, f.eks. generelle vejledninger og rammer for samtalen, som kan være både via RAG ("Retrieval-Augmented Generation") og indtastede prompts. Der vil også være generelle elementer, som beror på Børns Vilkårs generelle principper for samtaler med børn.

Den samlede løsning vil forventeligt også være i stand til at gemme historik på gennemførte samtaler og være i stand til at genoptage samtaleforløb. Det er fremadrettet et ønske at man vil kunne, diskutere samtaleforløbet med "coachbotten" efter endt samtale.

Det bemærkes, at ovenstående udgør en overordnet og foreløbig beskrivelse af de indledende projekttanker bag AI-løsningen. På tidspunktet for vejledningen var AI-løsningen fortsat under udvikling, og den endelige udformning var derfor ikke fastlagt. Der kan således forekomme ændringer i den videre udviklingsproces, som kan få betydning for de identificerede problemstillinger, casen har rejst i forhold til AI-forordningen og databeskyttelsesreglerne.

Oprindeligt var det hensigten, at Børns Vilkår selv ville udvikle samtalesimulatoren fremfor at bruge en ekstern leverandør. Børns Vilkår valgte imidlertid, efter at have fremsendt deres ansøgning om at

deltage i den regulatoriske sandkasse, at påbegynde arbejdet med at finde en leverandør, der kunne udvikle en AI-løsning med den ønskede systemfunktionalitet.

Ved sandkasseforløbets begyndelse var der ikke endeligt taget stilling til, hvilken leverandør der skulle udvikle løsningen. Derudover var AI-løsningen som udgangspunkt kun tiltænkt som et produkt, som Børns Vilkårs kunder skulle bruge i drift.

# 3. Databeskyttelsesretlige overvejelser

## 3.1. Indledning

Børns Vilkår ønsker som beskrevet ovenfor – i samarbejde med en ekstern leverandør – at udvikle en samtalesimulator, der ved brug af AI mulig gør det muligt for fagprofessionelle at træne samtaler med børn og unge i et simuleret fiktivt miljø. Børns Vilkår har under sandkasseforløbet oplyst, at Børns Vilkår ikke har til hensigt selv at anvende samtalesimulatoren men derimod sælge AI-løsningen til offentlige myndigheder og uddannelsesinstitutioner.

Drøftelserne i sandkasseforløbet tog udelukkende afsæt i Børns Vilkårs forpligtelser og ansvar efter databeskyttelsesreglerne i forbindelse med udviklingen/træningen og brugen af samtalesimulatoren. De offentlige myndigheders og uddannelsesinstitutionernes rolle blev alene drøftet overordnet, da formålet med sandkasseforløbet ikke har været at vurdere de offentlige myndigheders og uddannelsesinstitutionernes ansvar og forpligtelser efter databeskyttelsesreglerne i forbindelse med brugen af samtalesimulatoren.

I dette sandkasseforløb blev særligt personoplysningsbegrebet, herunder spørgsmålet om pseudonymisering og anonymisering, mulige retlige grundlag og rolle- og ansvarsfordeling drøftet.

## 3.2. Behandling af personoplysninger

Udvikling/træning og efterfølgende brug af en AI-løsning forudsætter som regel behandling af større datasæt.

Inden udvikling/træning eller indkøb og idriftsættelse af en AI-løsning påbegyndes, er det vigtigt at fastslå, om det datasæt, der benyttes, udgør personoplysninger, og dermed falder ind under databeskyttelsesforordningens anvendelsesområde. Det er en afgørende forudsætning for at kunne overholde databeskyttelsesreglerne.

Databeskyttelsesreglerne indeholder en bred definition af, hvad der udgør personoplysninger. Personoplysninger defineres som enhver form for information om en identificeret eller identificerbar fysisk person ('den registrerede').[4] Personoplysninger er altså enhver form for information, der kan henføres til en bestemt person, også selvom personen kun kan identificeres, hvis oplysningen kombineres med andre oplysninger.

Oplysninger, der er gjort anonyme, sådan at ingen fysiske personer kan identificeres ud fra oplysningerne eller i kombination med andre oplysninger, er ikke længere beskyttet af databeskyttelsesreglerne. Det skyldes, at databeskyttelsesreglerne kun finder anvendelse, så længe oplysningerne kan føres tilbage til en identificerbar eller identificeret fysisk person. Anonymisering er en proces, der sikrer, at data ikke kan knyttes til en fysisk person. Det er en betingelse, at anonymiseringen er uigenkaldelig og være lige så permanent som sletning, det vil sige gøre det umuligt at genidentificere den enkelte person.[5]

[4] Databeskyttelsesforordningens artikel 4, nr. 1.
[5] Artikel 29-gruppens udtalelse nr. 05/2014 om anonymiseringsteknikker (WP216), afsnit 2.1. Definitioner i EU-lovgivningen.

På samme måde er summarisk behandling af oplysninger om flere individer, som er blevet samlet og kombineret uden fokus på det enkelte individ, kun anonyme i det omfang der ikke er nogen, der kan genkende personerne ud fra oplysningerne eller i kombination med andre oplysninger. Dette kaldes ofte aggregerede oplysninger, og det vil bero på en konkret vurdering, om sådanne oplysninger er omfattet af databeskyttelsesreglerne.

Pseudonymisering er ikke en anonymiseringsmetode og kan derfor ikke sidestilles med anonymiserede data. Pseudonymisering gør det blot vanskeligere at koble datasættet til den enkelte persons identitet. Pseudonymiserede oplysninger anses derfor som udgangspunkt for personoplysninger efter databeskyttelsesforordningen, idet oplysningerne kan henføres til en identificerbar person, og er dermed omfattet af de forpligtelser, som følger af de databeskyttelsesretlige regler.

I forhold til en databehandlerkonstruktion vil personoplysninger, som er pseudonymiseret af den dataansvarlige, efter Datatilsynets opfattelse fortsat være personoplysninger, så længe oplysningerne behandles på den dataansvarliges vegne og efter dennes instruks, idet den dataansvarlige har nøglen, som fører retur til den registrerede.

I en databehandlerkonstruktion, kan enhver behandling udelukkende ske, fordi den dataansvarlige beslutter det, og den dataansvarlige har som sådan råderet over alle formål og midler, der skal benyttes. Databehandleren kan ikke – udenfor den dataansvarliges instruks – behandle personoplysningerne, og vurderingen skal derfor foretages fra den dataansvarliges perspektiv. Databehandlerens lovlige, tekniske eller kontraktuelle mulighed for at (re-)identificere de registrerede, er i dette scenarie ikke relevant for vurderingen af, om der er tale om personoplysninger, allerede fordi denne ikke må behandle det, der er personoplysninger – for den dataansvarlige – udover instruksen.[6]

### 3.2.1. Datasæt til udvikling/træning af samtalesimulatoren

*Barnebotten*

Børns Vilkår havde oprindeligt oplyst, at der ville ske træning af samtalesimulatoren med data fra Børns Vilkårs sms/chat-rådgivning på Børnetelefonen og de transskriberede data fra rådgivning via telefonen. Børns Vilkår oplyste i den forbindelse, at det var deres vurdering, at oplysningerne var anonymiserede.

I løbet af sandkasseforløbet oplyste Børns Vilkår imidlertid, at dette alligevel ikke var forventningen. Børns Vilkår har i den forbindelse oplyst, at barnebotten umiddelbart kan simulere et barn uden træning med data fra Børns Vilkår. Børns Vilkår har i den forbindelse oplyst, at Børns Vilkår – som beskrevet i ansøgningen til sandkasseforløbet – vil benytte transskriberede og anonymiserede data fra samtaler på Børnetelefonen, hvis der bliver behov for træningsdata.

Børns Vilkår beskrev i den forbindelse, at Børns Vilkår har opsat en datascrambler, der datavasker og sletter personoplysninger, således at optagede (mundtlige og skriftlige) samtaler på Børnetelefonen anonymiseres efter endt rådgivning.

[6] Sag C-413/23, *EDPS v. SRB* og Datatilsynets nyhedstekst af 22. oktober 2025 – mere nyt om EU-Domstolens afgørelse om pseudonymiserede personoplysninger.

*Coachbotten*

Børns Vilkår har indledningsvist i sandkasseforløbet oplyst, at Børns Vilkår vil udvikle og træne coachbotten med nogle samtaler i annoteret og anonymiseret form, og at samtalerne derfor ikke vil indeholde personoplysninger, der vil være omfattet af databeskyttelsesreglerne.

Børns Vilkår har efterfølgende til møderne oplyst, at Børns Vilkår udelukkende vil udvikle/træne coachbotten på tilgængeligt undervisningsmateriale i samtaler med børn udgivet af Børns Vilkår, og som ikke indeholder personoplysninger.

Nedenfor gennemgås Datatilsynets og Børns Vilkårs drøftelser af, hvornår oplysninger er anonymiseret eller pseudonymiseret.

### 3.2.2. Identifikationsvurderingen

Datatilsynet har i sandkasseforløbet understreget over for Børns Vilkår, at anvendelse af egne datasæt fra Børnetelefonen kræver en nøje vurdering af, om der er sket en reel og effektiv anonymisering.

Datatilsynet har i den forbindelse bemærket, at Børns Vilkår skal være opmærksom på, om Børns Vilkårs datasæt som oprindeligt har været omfattet af personoplysningsbegrebet rent faktisk er anonymiseret. Der er ikke tale om en absolut grænse mellem anonymiserede oplysninger og personoplysninger. Børns Vilkår skal derfor vurdere konkret, om Børns Vilkårs data reelt er anonymiseret på en så effektiv måde, at de registrerede ikke længere kan identificeres.

Ved vurderingen af om en person er identificerbar, skal Børns Vilkår tage alle hjælpemidler, der med rimelighed kan tænkes bragt i anvendelse, for at kunne identificere den enkelte person direkte eller indirekte, i betragtning. Børns Vilkår bør i vurderingen tage hensyn til bl.a. følgende objektive forhold[7]: Omkostninger ved og tid der er nødvendig til identifikation, under hensyntagen til den tilgængelige teknologi på behandlingstidspunktet og den teknologiske udvikling.

Datatilsynet og Børns Vilkår har drøftet personoplysningsbegrebet overordnet, herunder pseudonymisering og anonymisering af oplysninger. I den forbindelse har Datatilsynet henledt Børns Vilkårs opmærksomhed på, at Børns Vilkår – uanset om Børns Vilkår efter det oplyste anvender en datascrambler til at rense "personhenførbare" oplysninger fra samtalerne på Børnetelefonen – bør foretage en konkret vurdering af, hvorvidt der rent faktisk er sket en effektiv anonymisering af Børns Vilkårs datasæt. Børns Vilkår skal i den forbindelse vurdere, hvorvidt anonymiseringsprocessen er tilstrækkeligt robust, dvs. om identifikationen med rimelighed er blevet umuliggjort.

Børns Vilkår bør fokusere på de konkrete hjælpemidler, der skal bruges til at fjerne selve anonymiseringen, herunder de udgifter og den viden, der er nødvendig for kunne bruge hjælpemidlerne, og vurdere sandsynligheden for de enkelte personer kan (re)identificeres. Børns Vilkår bør f.eks. vurdere anonymiseringsindsatsen og omkostningerne både med hensyn til tid og ressourcer i forhold til, at der – i takt med den teknologiske udvikling – kommer flere mere tilgængelige tekniske hjælpemidler til at identificere personer i datasæt.[8]

Børns Vilkår bør derfor i forbindelse med brugen af datascrambleren være opmærksom på, at det bl.a. ikke vil være tilstrækkeligt kun at fjerne direkte identificerbare oplysninger for at sikre, at det ikke

[7] Databeskyttelsesforordningens betragtning 26.
[8] Artikel 29-gruppens udtalelse nr. 05/2014 om anonymiseringsteknikker (WP216), afsnit 2.2.2. muligheden for identifikation ved anonymiserede data.

længere muligt at identificere den enkelte person. Med en effektiv anonymisering vil ingen med rimelige hjælpemidler kunne koble oplysningerne i et datasæt til en person.

Datatilsynet har ikke taget stilling Børns Vilkårs eventuelle brug af data fra bl.a. samtaler på Børnetelefonen, herunder hvorvidt der er sket en effektiv anonymisering af Børns Vilkårs data, da Børns Vilkår ikke forventer at udvikle/træne samtalesimulatoren med egne datasæt.

## 3.3. Rolle- og ansvarsfordeling

I praksis kan det være svært at identificere, hvilke databeskyttelsesretlige roller de forskellige parter i en samarbejdsaftale har. I offentlig-private samarbejder om udvikling og anvendelse af AI-løsninger er det særligt vigtigt at være opmærksom på rollefordelingen, når der skal udveksles personoplysninger mellem parterne.

Allerede før parterne indgår i et formelt samarbejde, bør parterne forholde sig til deres roller efter databeskyttelsesreglerne, fordi kravene til dataansvarlige og databehandlere er forskellige. Som udgangspunkt er det den dataansvarlige, som har ansvaret for, at en behandling af personoplysninger lever op til reglerne i databeskyttelsesforordningen. Den dataansvarlige skal bl.a. sikre sig, at virksomheden:

- lovligt kan behandle de oplysninger, som den dataansvarlige og eventuelle databehandlere er i besiddelse af (dvs. om der er hjemmel til behandlingen),
- er i stand til at efterleve de registreredes personers rettigheder, og
- at eventuelle brud på persondatasikkerheden indberettes til Datatilsynet inden for 72 timer.

Hvis den dataansvarlige overlader personoplysninger til en databehandler, har den dataansvarlige endvidere et ansvar for, at databehandleren – på samme måde som den dataansvarlige selv – behandler oplysningerne forsvarligt. Den dataansvarlige skal i den forbindelse:

- sikre sig, at der er indgået en databehandleraftale med databehandleren, herunder at databehandleren er forpligtet til at bistå den dataansvarlige med at iagttage ovennævnte forpligtelser, og
- føre en passende kontrol med databehandleren.

Hvis parterne ikke på et tidligt stadie forholder sig til dette, er der risiko for, at projektet indrettes – både formelt og teknisk – på en måde, som forhindrer, at projektet kan gennemføres som planlagt. Der er derudover en risiko for, at ingen af parterne påtager sig ansvaret, eller at en part påtager sig et ansvar, som den pågældende reelt ikke har. Det er derfor meget vigtigt, at parterne – inden de begynder at behandle personoplysninger – får afklaret, hvilken rolle parterne har i forbindelse med behandlingen af personoplysningerne.

Parterne kan have forskellige roller i forhold til forskellige behandlingsaktiviteter i forbindelse med AI-projektet. Parterne skal derfor kortlægge og danne sig et overblik over samtlige behandlingsaktiviteter i projektet, både i forhold til udviklings- og træningsfasen samt driftsfasen.

Parterne skal indgå en databehandleraftale, når de har fundet ud af, hvem der er dataansvarlig og databehandler for de forskellige behandlingsaktiviteter. Databehandleraftalen skal leve op til kravene til databehandleraftaler i databeskyttelsesforordningen.[9] Det er vigtigt, at databehandleraftalen afspejler virkeligheden. Det vil sige, at parterne ikke kan beslutte en rollefordeling i forbindelse med

[9] Databeskyttelsesforordningens artikel 28, stk. 3.

behandling af personoplysninger, som ikke afspejler rollefordelingen i forhold til, hvem der reelt træffer alle væsentlige beslutninger om behandlingens formål og hjælpemidler.[10]

Samtalesimulatorprojektet er indrettet på en sådan måde, at Børns Vilkår i samarbejde med en IT-leverandør udvikler samtalesimulatoren[11], som offentlige myndigheder/uddannelsesinstitutioner (herefter kunder) skal anvende med henblik på at træne og kompetenceudvikle deres medarbejdere. Disse tre aktører har ikke fælles formål med behandlingen af oplysningerne, og indgår ikke som ligeværdige parter i en databeskyttelsesretlig kontekst.

Undervejs i sandkasseforløbet ændrede samtalesimulator-projektet sig væsentligt. Datatilsynets og Børns Vilkårs drøftelser har således været baseret på den viden, der forelå på tidspunktet af sandkasseforløbet, hvor projektet fortsat var i sin tidlige opstartsfase.

### 3.3.1. Databeskyttelsesretlige roller

*Dataansvarlig*

Inden for databeskyttelsesreglerne sondres der mellem bl.a. rollerne dataansvarlig og databehandler.

En dataansvarlig er den, der beslutter, hvorfor personoplysningerne skal behandles (afgør formål), og hvordan personoplysningerne skal behandles (afgør hjælpemidler). Det kan eksempelvis være en fysisk person, en juridisk person eller en offentlig myndighed.[12]

I forhold til hvilke hjælpemidler, der skal anvendes for at nå målet, sondres der mellem væsentlige og ikke-væsentlige hjælpemidler.

Væsentlige hjælpemidler er hjælpemidler, der er tæt forbundet med formålet og omfanget af behandlingen af personoplysninger, herunder hvilke typer af personoplysninger, der behandles, hvor længe personoplysningerne skal behandles, hvem der skal have adgang til personoplysningerne, og hvilke personers oplysninger behandles.[13] De væsentlige hjælpemidler er forbeholdt den dataansvarlige.

Ikke-væsentlige hjælpemidler vedrører mere praktiske aspekter af gennemførelsen, f.eks. valget af en bestemt type udstyr eller software eller de nærmere sikkerhedsforanstaltninger, som kan overlades til databehandleren at træffe beslutning om.

Den der beslutter de væsentligste elementer af databehandlingen, der sker som led i AI-projektet, vil være dataansvarlig for behandlingen af oplysningerne. Følgende spørgsmål kan bidrage til at afklare, om man beslutter "de væsentligste elementer" af behandlingen, og dermed pege i retning af, at man er dataansvarlig.

Hvis det er en anden part, der beslutter disse elementer, kan det tale i retning af, at denne er dataansvarlig.

[10] Datatilsynets vejledning af november 2017 om dataansvarlige og databehandlere, afsnit 3.1.2.
[11] Som beskrevet i afsnit 2 om projektbeskrivelsen.
[12] Databeskyttelsesforordningens artikel 4, nr. 7.
[13] EDPBs retningslinjer nr. 07/2020 for begreberne dataansvarlig og databehandler i den generelle forordning om databeskyttelse side 16.

Hvis man ikke bestemmer de væsentligste elementer, men stadig har en rolle i AI-projektet, kan det efter omstændighederne betyde, at man er databehandler.

**Beslutter I de væsentligste elementer?**

- Beslutter I, hvilken leverandør, der skal indgå i projektet, herunder i forhold til at udvikle AI-løsningen?
- Beslutter I, hvilke personoplysninger der skal behandles, og hvordan de skal behandles, herunder indsamles?
- Beslutter I, hvor længe personoplysningerne skal behandles, herunder om og hvornår oplysningerne skal slettes?
- Beslutter I, hvem personoplysningerne skal deles med?

*Databehandler*

En databehandler er en fysisk eller juridisk person, offentlig myndighed mv., der behandler personoplysninger på vegne af den dataansvarlige.[14] Databehandleren bestemmer i modsætning til den dataansvarlige, hverken hvorfor eller hvordan personoplysninger skal behandles. Databehandleren behandler alene oplysningerne efter den dataansvarliges instruks.

Den dataansvarlige kan overlade databehandleren en vis skønsmargin med hensyn til, hvordan den dataansvarliges interesser bedst varetages. Det indebærer, at databehandleren blandt andet kan vælge de mest velegnede tekniske og organisatoriske hjælpemidler til databehandlingen, uden at databehandleren herved bliver dataansvarlig.[15]

*Momenter af betydning vedrørende vurderingen af, om man er dataansvarlig*

Når det skal vurderes, hvem der er dataansvarlig og dermed har besluttet, hvorfor data behandles (afgør formål), og hvordan data behandles (afgør hjælpemidler), kan der som fortolkningsbidrag lægge vægt på nedenstående momenter.

Det er vigtigt at være opmærksom på, at momenterne kan pege i hver sin retning afhængigt af konteksten. Der vil således ikke altid kunne svares henholdsvis "ja" eller "nej" til alle spørgsmål. I disse tilfælde må momenterne holdes op mod hinanden i vurderingen af, hvilken konstruktion der er flest og mest tungtvejende momenter for.

Vurderingen af de databeskyttelsesretlige roller bør angå hver enkelt aktivitet. Det betyder, at en aktør kan være selvstændig dataansvarlig for én del af behandlingsaktiviteterne, men være databehandler for en anden del.

Hvis der ikke kan siges "ja" til nogen af nedenstående spørgsmål, kan det pege i retning af, at den pågældende aktør er databehandler. Dette gælder også, selvom aktøren træffer visse beslutninger i relation til AI-projektet og dets udførelse.

- *Følger forpligtelsen af lov*
  Det kan være fastsat i lovgivningen, at en organisation er dataansvarlig eller forpligtet til at behandle udvalgte typer af personoplysninger til nærmere angivne formål.

[14] Databeskyttelsesforordningens artikel 4, nr. 8.
[15] EDPBs retningslinjer nr. 07/2020 for begreberne dataansvarlig og databehandler i den generelle forordning om databeskyttelse side 3.

Hvis det er tilfældet, vil den pågældende aktør være dataansvarlig for den behandling, som sker på baggrund af forpligtelsen, eller fordi det fremgår direkte af loven.

I andre tilfælde kan lovgivningen indeholde mere generelle bestemmelser, som pålægger aktøren at udføre en overordnet opgave. Lovgivningen vil derved efterlade et større råderum for, hvordan oplysningerne skal behandles og derved ikke entydigt pege på, om man er dataansvarlig eller ej.

- *Er der taget initiativ til AI-projektet*
  Hvis det ikke er fastsat i lovgivningen, at en organisation er dataansvarlig eller forpligtet til at behandle udvalgte typer af personoplysninger til nærmere angivne formål, skal vurderingen fastlægges på grundlag af de faktiske omstændigheder i forbindelse med behandlingen.

  Hvis organisationen er initiativtager til et AI-projekt, kan det tale for, at den pågældende organisation er dataansvarlig. Det skyldes, at den part, som tager initiativ til AI-projektet, ofte vil være med til at fastlægge rammerne for projektet.

  I vurderingen skal der lægges vægt på de enkelte behandlingsaktiviteter, herunder hvem der beslutter, hvorfor og hvordan personoplysninger behandles i forbindelse med AI-projektet. Det gælder både for så vidt angår udviklings- og driftsfasen.

### 3.3.2. Rollefordeling i forhold til samtalesimulator

I sandkasseforløbet har det været drøftet, hvilke databeskyttelsesretlige roller Børns Vilkår har i forhold til IT-leverandøren og kunderne. Det har bl.a. været drøftet, hvornår Børns Vilkår er henholdsvis databehandler og dataansvarlig. Børns Vilkår har i den forbindelse kortlagt Børns Vilkårs og de øvrige aktørers rolle- og ansvarsfordeling på tværs af de forskellige procestrin i udviklingen og driften af samtalesimulatoren. På den baggrund har det været drøftet, hvilken databeskyttelsesretlig rolle Børns Vilkår vil have i forhold til de forskellige procestrin.

**Procestrin: Konfiguration/prompting af samtalesimulatoren**

Børns Vilkår har i forhold til konfigurering af samtalesimulatoren oplyst, at Børns Vilkår ikke vil bruge data, der er personhenførbare, men alene data som vedrører systemopsætning og performance.

Formålet med brugen af disse data er at initialisere AI-systemet med foruddefinerede prompts og strukturerede input til simulerede cases.

Det har ikke været en del af drøftelserne i sandkasseforløbet, om Børns Vilkårs rolle- og ansvarsfordeling for så vidt angår konfigurering af samtalesimulatoren, idet der ikke vil ske behandling af personoplysninger i forbindelse med konfigurering/prompting af samtalesimulatoren. Hvis Børns Vilkår derimod anvender personoplysninger som led i konfiguration/prompting af samtalesimulatoren, vil Børns Vilkår umiddelbart være dataansvarlig for disse behandlingsaktiviteter, hvis Børns Vilkår bestemmer hvorfor og hvordan personoplysningerne behandles.[16]

[16] Der henvises til afsnit 3.3.1 og 3.3.2 om definition og vurdering.

### Procestrin: Supplerende træning af samtalesimulatoren (barnebotten)

Børns Vilkår har i sandkasseforløbet oplyst, at Børns Vilkår som udgangspunkt ikke forventer at udvikle og træne samtalesimulatoren, herunder barnebotten, med data fra Børnetelefonen, medmindre der opstår et udtalt behov for det. Der vil i så fald kun være tale om anonymiseret data fra Børnetelefonen i form af anonymiserede mundtlige (transskriberede) og skriftlige samtaler fra Børnetelefonen, der skal indgå i udviklings- og træningsdatasættet. Udvikling og træning af samtalesimulatoren vil dermed ikke ske på personhenførbare oplysninger, og aktiviteterne i dette procestrin vil derfor ikke være omfattet af de databeskyttelsesretlige regler.

Formålet med Børns Vilkårs eventuelle brug af supplerende data fra Børnetelefonen er at forbedre realismen og responskvaliteten af barnebotten.

Datatilsynet har henledt Børns Vilkårs opmærksomhed på forskellen mellem pseudonymisering og anonymisering i en databeskyttelsesretlig kontekst.[17] Datatilsynet har i den sammenhæng oplyst, at vurdering af pseudonymisering og anonymisering er en forudsætning for at afklare om, der skal identificeres en hjemmel til bl.a. behandling af eventuelle (pseudonymiserede) personoplysninger i forbindelse med udvikling af samtalesimulatoren og i den forbindelse også kortlægning af dataansvaret og datastrømmene.

Da Børns Vilkår ikke forventer at udvikle og træne samtalesimulatoren med data fra Børnetelefonen, blev dette procestrin ikke drøftet yderligere.

### Procestrin: Adgangskontrol i forhold til systemadgange og licenser

Børns Vilkår har i sandkasseforløbet oplyst, at formålet med adgangskontrollen er at administrere systemadgangsrettighederne og licenserne overfor deres kunder. Autentificeringen af medarbejderne hos kunden sker gennem Single Sign ON (SSO)[18]via kundens Identity Provider (IdP).[19] På den måde kan Børns Vilkår sikre, at kun kunder, der har indgået en aftale med Børns Vilkår, er aktive og har adgang til samtalesimulatoren.

Børns Vilkår har desuden oplyst, at adgangskontrollen er centraliseret med det formål, at Børns Vilkår kan bevare styringen over adgangskontrollen, som de ønsker. I forbindelse med adgangsstyringen til samtalesimulatoren vil der bl.a. blive indsamlet oplysninger om kundens medarbejders navn, arbejds-e-mail, medarbejderens titel og arbejdsplads.

De relevante overvejelser i forhold til rolle- og ansvarsfordelingen mellem Børns Vilkår, kunden og IT-leverandøren er, hvem der beslutter hvorfor og hvordan personoplysningerne skal behandles i forbindelse med adgangskontrollen i forhold til systemadgangen og licenser til samtalesimulatoren.

Det er blevet drøftet, at Børns Vilkår vil kunne anses som dataansvarlig for behandlingen af oplysninger om bl.a. kundens medarbejders navn og arbejds-e-mail i forbindelse med adgangskontrollen til at tilgå samtalesimulatoren, herunder licensstyring, hvis det er Børns Vilkår der beslutter hvorfor og hvordan personoplysningerne skal indsamles, herunder hvilke typer af personoplysninger, der skal indsamles, hvor længe personoplysningerne skal behandles, og hvem der skal have adgang til personoplysningerne.

[17] Der henvises til afsnit 3.2 om pesudonymisering og anonymisering.
[18] En fællesbetegnelse for en funktionalitet, hvor du kun skal logge ind én gang, for at få adgang til flere forskellige systemer. Ideen er typisk at øge sikkerheden, ved at der kun skal anvendes ét sæt adgangsgivende oplysninger (f.eks. brugernavn/password). En anden fordel er at adgang til systemer dermed kan ændres og fjernes mere centralt.
[19] En tjeneste der bekræfter, hvem du er, når du logger ind. Det fungerer som digital legitimation, så andre systemer dermed kan stole på din identitet.

### Procestrin: Bruger- og brugsoplysninger

I forhold til brugeroplysninger har Børns Vilkår oplyst, at der, efter login i samtalesimulatoren, behandles profiloplysninger om kundens medarbejdere – i form af navn, titel og arbejdsplads – fra SSO-tokens[20]. Behandlingen af disse personoplysninger er udelukkende begrænset til identifikationsformål og med henblik på at føre revision og audit.

I forhold til brugsoplysninger har Børns Vilkår oplyst, at der indsamles og behandles stemme- og tekstoplysninger om kundens medarbejdere via medarbejdernes tekst og tale input til samtalesimulatoren, når samtalesimulatoren er i brug hos en kunde. Disse oplysninger videregives til barnebotten, der er understøttet af en GPT-model[21], og som herefter generer et svar eller en reaktion til kundens medarbejdere. Under og efter samtalen generer coachbotten, som også er understøttet af en GPT-model, feedback baseret på den samtale, kundens medarbejdere har haft med barnebotten.

Børns Vilkår har desuden oplyst, at inputtet, som indeholder personoplysninger i form af stemme og tekst, behandles af en GPT-model i et lukket system. Børns Vilkår har efterfølgende oplyst, at stemmedata behandles transient, hvilket betyder, at data kun eksisterer under transskriberingsprocessen og ikke lagres efterfølgende. Udgangspunktet er, at hverken Børns Vilkår eller IT-leverandøren vil eller kan anvende disse personoplysningerne til at træne samtalesimulatoren eller til øvrige formål.

Derudover har Børns Vilkår i sandkasseforløbet oplyst, at Børns Vilkår ikke har adgang til ovennævnte oplysninger, og at oplysningerne strømmer direkte fra kunden til IT-leverandøren.

Datatilsynet og Børns Vilkår har drøftet de mulige scenarier i forhold til rollefordelingen mellem Børns Vilkår, kunden og IT-leverandøren vedrørende bruger- og brugsoplysninger. I den sammenhæng hvor kunden beslutter at anvende samtalesimulatoren til læring og træning af deres medarbejdere med henblik på at forbedre rådgivningen til børn og unge, vil kunden umiddelbart anses som dataansvarlig. Kunden bestemmer, hvilke medarbejdere og hvilke oplysninger om medarbejderne der skal anvendes, og hvilke hjælpemidler der skal bruges i forbindelse med brugen af samtalesimulatoren. IT-Leverandøren vil i den forbindelse være databehandler for kunden, idet IT-leverandøren kun står for driftsdelen, herunder de tekniske hjælpemidler med henblik på at skabe den nødvendige sikkerhed.

Ud fra den ovennævnte konstruktion, vil der være tale om en rolle- og ansvarsfordeling, hvor kunden er dataansvarlig og IT-leverandøren er databehandler.

På baggrund af drøftelserne har Datatilsynet vejledt Børns Vilkår om, at Børns Vilkår – som ønsker at være bindeled mellem kunden og IT-leverandøren for så vidt angår bruger- og brugsoplysninger – kan overveje at udlicitere driftsdelen til IT-leverandøren, således at Børns Vilkår som databehandler anvender IT-leverandøren som underdatabehandler.

Børns Vilkår skal imidlertid være opmærksom på, at Børns Vilkår ikke må gøre brug af en anden databehandler uden forudgående specifik eller generel skriftlig tilladelse fra kunden.[22] Børns Vilkår skal i den forbindelse sørge for at indhente kundens skriftlige godkendelse før underdatabehandleren (IT-leverandøren) får overdraget driftsdelen. Derudover skal Børns Vilkår indgå en kontrakt med IT-

[20] En unik digital nøgle eller unik tekststreng, som identificerer dig overfor de systemer du vil logge ind via Single Sign On. Den bruges typisk til at bevise overfor systemer, at du allerede er retmæssigt logget ind ét sted, og dermed ikke behøves logge ind igen.
[21] En neural netværksmodel, der er trænet på store mængder tekst. Modellen er trænet til at forudsige næste ord i en sekvens. Den bruger mønstre i data til at generere sammenhængende tekst, besvare spørgsmål og andre opgaver på basis af sandsynlighedsberegninger.
[22] Databeskyttelsesforordningens artikel 28, stk. 2.

leverandøren, hvori IT-leverandøren pålægges de samme forpligtelser, som Børns Vilkår selv er underlagt over for kunden.[23]

Børns Vilkår skal – udover hvad der fremgår af kontrakten mellem Børns Vilkår og IT-leverandøren – være opmærksom på, at de faktiske omstændigheder skal indrettes på en måde, som afspejler det, som formelt aftales.

Børns Vilkår skal desuden være opmærksom på, om IT-leverandøren viderebehandler personoplysninger til egne formål. Børns Vilkår bør sikre, at IT-leverandørens behandling af personoplysninger sker i overensstemmelse med databehandleraftalen. Det vil derfor være relevant at være opmærksom på dataflowet, herunder hvad leverandøren umiddelbart ville have adgang til.

I tilfælde af at IT-leverandøren ønsker at viderebehandle personoplysninger til egne formål, skal kunden sikre, at der er hjemmel til at videregive personoplysninger til IT-leverandøren med henblik på, at leverandøren kan behandle personoplysninger til egne formål. Kunden skal således sikre, at der er hjemmel i lyset af alle de formål, som personoplysningerne skal videregives til.[24] Derudover skal IT-leverandøren sikre, at der er hjemmel til at indsamle og behandle oplysningerne.

Det er derfor vigtigt, at Børns Vilkår allerede nu går i dialog med IT-leverandøren i forhold til, hvilke metadata IT-leverandøren ønsker at bruge og til hvilke formål. Det er også tilfældet, hvis IT-leverandøren alene ønsker at bruge generiske data, som ikke kan henføres til kundens enkelte medarbejdere.

### Procestrin: Aggregeret data og KPI'er

Børns Vilkår har oplyst, at de ønsker at bruge aggregeret data og KPI'er[25] til løbende at videreudvikle og prompte samtalesimulatoren. Hvis de aggregerede data og KPI'er indeholder personoplysninger, og hvis der i forbindelse heraf sker behandling af personoplysninger, vil de databeskyttelsesretlige regler finde anvendelse.

Typiske KPI'er vil kunne omfatte følgende oplysninger:

- Tidspunkt for kundens medarbejderes brug af samtalesimulatoren og varighed af sessionen.
- Antal forsøg eller gentagelse pr. træningsscenarie.
- Forbedringer i systemets kvantitative evalueringsmetrikker (udtrykt som procentvis forbedring og aggregerede summeringer)
- Oversigt over de mest udbredte brugervanskeligheder (aggregerede brugerdata)
- Brugstal for nøgle systemfunktioner
- Yderligere anonymiserede indikatorer for brugeraktivitet og læringsresultater

Børns Vilkår har i forhold til procestrinnet oplyst, at der i selve samtalesimulator-løsningen vil være defineret et sæt KPI'er for hver kundeinstallation. Børns Vilkår har derudover oplyst, at alle KPI-data anonymiseres eller aggregeres før analyserne, og at det ikke indeholder personhenførbare oplysninger om de enkelte medarbejdere hos kunden.

I oversigten nedenfor fremgår formålet med de forskellige aktørers brug af KPI'er:

23 EDPBs retningslinjer 07/2020 for begreberne dataansvarlig og databehandler i den generelle forordning om databeskyttelse, afsnit 1.3.4
24 Dette var også et centralt tema Datatilsynets afgørelse i sagen med j.nr. 2025-431-0053 (den såkaldte Chromebook-sag).
25 Key Performance Indicators.

| | |
|---|---|
| **Børns Vilkårs brug af KPI'er** | KPI-resuméer bruges til at dokumentere effekten af læringssystemet og til at designe og forfine nye læringsscenarier. Børns Vilkår analyserer anonymiserede data for at identificere generelle tendenser, vurdere pædagogiske resultater og forbedre uddannelseskvaliteten på tværs af kundeimplementeringer |
| **Leverandørens brug af KPI'er** | Bruger anonymiserede KPI-data til videreudvikling og optimering af samtalesimulatoren. Leverandøren vil kun bruge aggregerede brugsmønstre og funktionsudnyttelse for at identificere, hvor systemfunktionaliteten kan forbedres, optimeres eller udvides. Leverandøren har ikke adgang til personlige læringsdata eller identificerbar brugeradfærd. |
| **Kundeorganisationens brug af KPI'er** | Hver leder/vejleder i kundeorganisationen kan modtage en begrænset delmængde af KPI'er, der fokuserer på læringsresultater på teamniveau. Disse målinger hjælper med at illustrere effekten af uddannelsesinitiativer og henlede opmærksomheden på læringsemner, der konsekvent præsenterer udfordringer. Ingen individuel præstationsevaluering deles med andre end slutbrugeren. Der er fortsat fokus på overvågning af kollektive fremskridt og funktionsudvikling. |

Datatilsynet og Børns Vilkår har bl.a. drøftet Børns Vilkårs databeskyttelsesretlige rolle i tilfælde af, at der ikke er tale om anonymiserede data.

Børns Vilkår har i forlængelse heraf identificeret sig selv som databehandler og IT-leverandøren som underdatabehandler i forhold til kunderne, som Børns Vilkår vurderer, er dataansvarlige. Børns Vilkår har i den forbindelse oplyst, at Børns Vilkår og/eller IT-leverandøren (databehandler/underdatabehandler) kun ønsker at anvende anonymiseret data i forbindelse med at videreudvikle og træne samtalesimulatoren.

Når der behandles personoplysninger i forbindelse med de aggregerede data og KPI'er med henblik på at udvikle og træne AI-løsningen, er det imidlertid vigtigt at være opmærksom på, hvilket formål de aggregerede data og KPI'er er indsamlet til, herunder om disse data er skabt til brug for Børns Vilkår eller kunden. Hvis det er kunden, der ønsker at bruge KPI'er og de aggregerede data til f.eks. at måle de enkelte medarbejdere, vil det således være kunden, der er dataansvarlig for denne behandling. Hvis det derimod er Børns Vilkår og/eller It-leverandøren, der ønsker at bruge aggregeret data og KPI'er til egne formål – f.eks. til videreudvikling af løsningen – vil det være Børns Vilkår og/eller IT-leverandøren, som bliver dataansvarlig.

Det er derfor vigtigt at fokusere på, til hvis formål de aggregerede data og KPI'er bliver skabt.

Datatilsynet har i forlængelse heraf henledt Børns Vilkårs opmærksomhed på, at der i en databehandlerkonstruktion mellem kunden og Børns Vilkår og/eller IT-leverandøren vil være identifikation mellem

kunden og Børns Vilkår og/eller IT-leverandøren, da Børns Vilkår og/eller it-leverandøren bl.a. kun må behandle personoplysninger i overensstemmelse med den afgivne instruks.[26]

I en databehandlerkonstruktion mellem kunden, Børns Vilkår og/eller IT-leverandøren vil personoplysninger, som er pseudonymiseret af kunden fortsat være personoplysninger, så længe oplysningerne behandles på kundens vegne og efter dennes instruks, idet kunden ved brug af supplerende oplysninger vil kunne identificere de enkelte medarbejdere.[27]

Hvis Børns Vilkår og/eller IT-leverandøren som databehandler og/eller underdatabehandler ønsker at behandle aggregeret data på baggrund af data, der er pseudonymiseret af kunden, til egne formål, herunder videreudvikling og træning af samtalesimulatoren, vil det således følge af databehandlerkonstruktionen, at oplysningerne fortsat vil være personoplysninger for kunden, som dataansvarlig. Kunden skal derfor have hjemmel i databeskyttelsesforordningens artikel 6, stk. 1, til at videregive disse data til Børns Vilkår og/eller IT-leverandøren, der er den nye dataansvarlig i forhold til dennes egne formål. Det gælder uanset, om oplysningerne i den nye behandlingskontekst efter omstændighederne vil kunne falde uden for definitionen af, hvad der er en personoplysning. Hvis Børns Vilkår ønsker at anvende data til at videreudvikle og træne samtalesimulatoren, bliver Børns Vilkår selvstændigt dataansvarlig for indsamlingen og skal også finde et særskilt retsgrundlag for dette.

**Procestrin: Børns Vilkårs egen interne brug af samtalesimulatoren**

Hvis Børns Vilkår ønsker at anvende samtalesimulatoren til at uddanne Børns Vilkårs egne børne- og ungerådgivere, bliver Børns Vilkår selvstændigt dataansvarlig for behandlingen af personoplysninger i den forbindelse. Dette blev ikke drøftet yderligere, idet Børns Vilkår som udgangspunkt ikke ønsker at anvende samtalesimulatoren til internt brug.

## 3.4. Retligt grundlag

Udvikling/test og drift af en AI-løsning er typisk en iterativ proces, der består af en række forskellige faser, som ikke nødvendigvis følger en bestemt rækkefølge. Det er en grundlæggende forudsætning for, at der lovligt kan behandles personoplysninger i forbindelse med udvikling/test og efterfølgende brug af en AI-løsning, at der for hvert formål er identificeret et behandlingsgrundlag. Der bør derfor indledningsvist foretages en samlet vurdering af livscyklussen.

Ved vurderingen af mulige behandlingsgrundlag bør der sondres mellem behandling af personoplysninger i forbindelse med udvikling/test og den efterfølgende drift af AI-løsningen. Det skyldes, at der i en databeskyttelsesretlig kontekst er tale om forskellige formål, og behandlingen af personoplysninger kan derfor ikke nødvendigvis baseres på det samme behandlingsgrundlag.

Børns Vilkår vil – som nævnt ovenfor – behandle personoplysninger i forbindelse med Børns Vilkårs eventuelle interne brug af samtalesimulatoren, og når samtalesimulatoren er i brug hos kunden. Børns Vilkår forventer derimod ikke at behandle personoplysninger i forbindelse med udviklingen af løsningen. Derfor gennemgås mulige retlige grundlag i udviklings- og træningsfasen derfor ikke i dette afsnit.[28]

Databeskyttelsesforordningens artikel 6, stk. 1, litra a-f, udgør en udtømmende liste af retlige grundlag. Behandling af personoplysninger er kun lovlig, hvis mindst ét af de oplistede forhold gør sig

[26] Se afsnit 3.2 om behandling af personoplysninger, hvor der redegøres for dette.
[27] Se afsnit 3.2 om behandling af personoplysninger, sag C-413/23, EDPS v. SRB og Datatilsynets hjemmeside: Mere nyt om EU-Domstolens afgørelse om pseudonymiserede personoplysninger
[28] Se de forskellige procestrin under afsnit 3.3

gældende. De forskellige retlige grundlag er ligestillede, og der er derfor ikke noget retligt grundlag, der går forud for andre. Det er dog vigtigt, at man som dataansvarlig overvejer, hvilket retligt grundlag der er det mest passende at basere sin behandling på i forhold til formålet med behandlingen af oplysningerne.

I dette sandkasseforløb er de forskellige mulige behandlingsgrundlag for Børns Vilkårs behandling af personoplysninger blevet drøftet overordnet, da samtalesimulator-projektet på tidspunktet for sandkasseforløbet kun var i opstartsfasen.

Drøftelserne tog udgangspunkt i behandlingsgrundlagene for den behandling af personoplysninger, som Børns Vilkår ønsker at foretage i forbindelse med følgende procestrin: adgangskontrol i forhold til systemadgange og licenser, aggregeret data og KPI'er samt Børns Vilkårs egen interne brug af samtalesimulatoren.

Børns Vilkår har under sandkasseforløbet peget på databeskyttelsesforordningens artikel 6, stk. 1, litra f[29], som retligt grundlag for så vidt angår Børns Vilkårs behandlingsaktiviteter i forbindelse med adgangskontrol, hvor formålet med adgangskontrollen er at administrere systemadgangsrettighederne og licenserne overfor deres kunder. Det samme retlige grundlag har Børns Vilkår peget på i forhold til deres eventuelle interne brug af samtalesimulatoren. Børns Vilkår har imidlertid ikke peget på et behandlingsgrundlag for så vidt angår behandling af aggregeret data og KPI'er til løbende at videreudvikle og træne samtalesimulatoren.

Datatilsynet har i sandkasseforløbet henledt Børns Vilkårs opmærksomhed på, at anvendelse af artikel 6, stk. 1, litra f, kræver en vurdering af, om behandlingen af oplysningerne i forbindelse med adgangskontrol, herunder licensstyring, og Børns Vilkårs egen interne brug af samtalesimulatoren med henblik på at kompetenceudvikle egne medarbejdere/frivillige rådgivere er nødvendig for, at Børns Vilkår kan forfølge en legitim interesse, som ikke kan overgås af de registreredes grundlæggende interesser og frihedsrettigheder.

Datatilsynet har desuden bemærket, at det også kan være hensigtsmæssigt at undersøge, om databeskyttelsesforordningens artikel 6, stk. 1, litra b[30] og c[31] kan anvendes som behandlingsgrundlag i forhold til Børns Vilkårs behandling af oplysninger i forbindelse med Børns Vilkårs interne brug af samtalesimulatoren. Disse behandlingsgrundlag kan også være relevante at undersøge i forhold til når Børns Vilkår foretager adgangskontrol af deres kunder i forbindelse med brugen af samtalesimulatoren.

Børns Vilkårs formål med behandlingen af personoplysninger i forbindelse med adgangskontrol er at administrere systemadgangsrettighederne og licenserne over for deres kunder, herunder sikre, at kun kunder, der har indgået en aftale med Børns Vilkår, er aktive og har adgang til samtalesimulatoren.

Børns Vilkårs formål med behandlingen af personoplysninger i forbindelse med Børns Vilkårs interne brug er at sikre den fornødne kompetenceudvikling for Børns Vilkårs medarbejdere/frivillige rådgivere.

Når de databeskyttelsesretlige problemstillinger drøftes i et sandkasseforløb, er det en del af processen, at deltagerne udfordres på de vurderinger, de har foretaget – bl.a. om behandlingsgrundlag. Det

[29] Databeskyttelsesforordningens artikel 6, stk. 1, litra f: *Behandling er nødvendig for, at den dataansvarlige eller en tredjemand kan forfølge en legitim interesse, medmindre den registreredes interesser eller grundlæggende rettigheder og frihedsrettigheder, der kræver beskyttelse af personoplysninger, får forud herfor, navnlig hvis den registrerede er et barn.*

[30] Databeskyttelsesforordningens artikel 6, stk. 1, litra b: *Behandling er nødvendig af hensyn til opfyldelse af en kontrakt, som den registrerede er part i, eller af hensyn til gennemførelse af foranstaltninger, der træffes på den registreredes anmodning forud for indgåelse af en kontrakt*

[31] Databeskyttelsesforordningens artikel 6, stk. 1, litra c: Behandling er nødvendig for at overholde en retlig forpligtelse, som påhviler den dataansvarlige.

er for at hjælpe deltagerne til at foretage en grundig dokumenteret vurdering af de forskellige problemstillinger. I forhold til valg af behandlingsgrundlag er det derfor i mange tilfælde relevant for Datatilsynet at høre om deltagernes overvejelser om forskellige mulige behandlingsgrundlag. Det er for at hjælpe på vej i en vurdering af, hvilket behandlingsgrundlag der er mest hensigtsmæssigt i forhold til deres behandling af personoplysninger i de forskellige faser af et AI-projekt.

Datatilsynet har i sandkasseforløbet ikke taget stilling til, hvilket/hvilke behandlingsgrundlag der er det/de rette. Datatilsynet og Børns Vilkår har imidlertid overordnet drøftet de forskellige krav til anvendelse af databeskyttelsesforordningens artikel 6, stk. 1, litra b, c og f.

### 3.4.1. Kontrakt

Databeskyttelsesforordningens artikel 6, stk. 1, litra b, kan anvendes som behandlingsgrundlag, hvis behandlingen af personoplysninger i forbindelse med at kompetenceudvikle medarbejdere/frivillige rådgivere er en nødvendig af hensyn til arbejdsgiverens opfyldelse af kontrakten mellem Børns Vilkår og deres medarbejdere/frivillige rådgivere.

Det betyder, at behandling af personoplysninger om medarbejdere/frivillige rådgivere i forbindelse med kompetenceudvikling vil kunne ske på baggrund af en kontrakt, hvis betingelserne for det er opfyldt.

Databeskyttelsesforordningens artikel 6, stk. 1, litra b, finder anvendelse, hvis én af to betingelser er opfyldt: 1) Behandlingen skal være objektivt nødvendig af hensyn til opfyldelsen af en kontrakt med en registreret, eller 2) behandlingen skal være objektivt nødvendig af hensyn til gennemførelsen af foranstaltninger forud for kontrakten på anmodning af en registreret.

Databeskyttelsesforordningens artikel 6, stk. 1, litra b, skal tages i betragtning i sammenhæng med databeskyttelsesforordningen i dens helhed, herunder særligt med dataansvarliges pligt til at behandle personoplysninger lovligt, rimeligt og på en gennemsigtig måde i forhold til den registrerede. Princippet om rimelighed omfatter bl.a. anerkendelse af rimelige forventninger hos den registrerede, overvejelse af eventuelle negative konsekvenser, som behandlingen kan have for dem, og inddragelse af forhold og potentielle virkninger af ubalance mellem dem og den dataansvarlige.[32]

Børns Vilkår skal vurdere, om selve behandlingen af personoplysninger i forbindelse med kompetenceudvikling af medarbejdere/frivillige rådgivere er nødvendig af hensyn til Børns Vilkårs opfyldelse af ansættelseskontrakten med medarbejderne/frivillige rådgivere.

Nødvendighedskravet i databeskyttelsesforordningens artikel 6, stk.1, litra b, skal fortolkes strengt. Det vil derfor ikke omfatte de situationer, hvor behandlingen ikke reelt er nødvendig af hensyn til opfyldelse af en kontrakt.[33]

Hvis der alene er tale om et tilbud i forhold til selve brugen af samtalesimulatoren med henblik på at udvikle ens kompetencer inden for rådgivning af børn og unge, som medarbejdere/frivillige rådgivere kan vælge ikke at bruge, vil det umiddelbart tale for, at databeskyttelsesforordningens artikel 6, stk. 1, litra b, ikke kan anvendes.

[32] EDPBs Retningslinjer 2/2019 for behandling af personoplysninger i henhold til artikel 6, stk. 1, litra b), i GDPR i forbindelse med leveringen af onlinetjenester til registrerede, afsnit 2.1.
[33] EDPBs Retningslinjer 2/2019 for behandling af personoplysninger i henhold til artikel 6, stk. 1, litra b), i GDPR i forbindelse med leveringen af onlinetjenester til registrerede, afsnit 2.5.

### 3.4.2 Retlig forpligtelse

I forhold til Børns Vilkårs ønske om at behandle personoplysninger i forbindelse med adgangskontrol og licensstyring, kan det være hensigtsmæssigt at undersøge, om databeskyttelsesforordningens artikel 6, stk. 1, litra c, kan anvendes som lovligt behandlingsgrundlag.

For at databeskyttelsesforordningens artikel 6, stk. 1, litra c, skal kunne anvendes som behandlingsgrundlag, skal behandlingen have et supplerende retsgrundlag. Databeskyttelsesforordningens artikel 6, stk. 3, indeholder flere krav til det supplerende retsgrundlag.

Det er et krav efter artikel 6, stk. 1, 1. pkt., at grundlaget for behandlingen skal fremgå af EU-retten eller national ret, som den dataansvarlige er underlagt.

Datatilsynet har overordnet henledt Børns Vilkårs opmærksomhed på, at det er relevant at vurdere, hvorvidt Børns Vilkårs behandling af personoplysninger i forbindelse adgangskontrol og licensstyring vil være nødvendig for, at Børns Vilkår kan overholde de retlige forpligtelser, som påhviler Børns Vilkår til at sikre et passende sikkerhedsniveau i løsningen.[34] Dette forudsætter selvfølgelig, at formålet med behandlingen sker med henblik på at forbedre sikkerheden i og pålideligheden af samtalesimulatoren.

### 3.4.3 Interesseafvejning

Børns Vilkår baserer som nævnt ovenfor sin behandling af personoplysninger for så vidt angår adgangskontrol og licensstyring af kunderne og Børns Vilkårs egen interne brug af samtalesimulatoren med henblik på at kompetenceudvikle egne medarbejdere/frivillige rådgivere på databeskyttelsesforordningens artikel 6, stk. 1, litra f.

Datatilsynet har som nævnt ovenfor henledt Børns Vilkårs opmærksomhed på, at anvendelse af artikel 6, stk. 1, litra f, generelt kræver en konkret vurdering af, om behandlingen af personoplysninger i forbindelse med de to formål er nødvendig for, at Børns Vilkår kan forfølge en legitim interesse, som ikke overgås af de registreredes grundlæggende interesser og frihedsrettigheder. En sådan vurdering skal i øvrigt dokumenteres.[35]

Der er tre kumulative krav, der alle skal være opfyldt, før bestemmelsen om interesseafvejningen kan anvendes som lovligt behandlingsgrundlag.

#### 1) Legitim interesse

**For det første** skal behandlingen forfølge den dataansvarliges eller tredjeparts interesse. Der er tale om en legitim interesse, hvis interessen er 1) lovlig, 2) klar og præcist formuleret og 3) reel og aktuel – ikke spekulativ.[36]

#### 2) Behandlingens nødvendighed

**For det andet** skal der foretages en vurdering af, om behandlingen af personoplysninger er nødvendig i forhold til den legitime interesse, der forfølges. Vurderingen indeholder to elementer: 1) om

[34] En sådan forpligtelse følger bl.a. af databeskyttelsesforordningens artikel 32, hvorefter der ved behandling af personoplysninger skal gennemføres passende tekniske og organisatoriske foranstaltninger for at sikre et sikkerhedsniveau, der passer til de risici behandlingen af personoplysninger indebærer for de registrerede. Det kan være nødvendigt at behandle personoplysninger i forbindelse med implementering af forskellige typer sikkerhedsforanstaltninger, bl.a. adgangskontrol.

[35] I overensstemmelse med artikel 5, stk. 2, skal den dataansvarlige kunne påvise, at artikel 5, stk. 1, overholdes, herunder kravet i artikel 5, stk. 1, litra a om, at personoplysninger skal behandles lovligt, rimeligt og på en gennemsigtig måde i forhold til den registrerede.

[36] EDPBs vejledning nr. 1/2024 om behandling af personoplysninger baseret på artikel 6, stk. 1, litra f.

behandlingsaktiviteten vil gøre det muligt at forfølge formålet, og 2) om der er nogle mindre indgribende måder at forfølge dette formål på.[37]

Omfanget af personoplysninger skal tages i betragtning i vurderingen af nødvendigheden af behandlingen både i forhold til Børns Vilkårs interne brug af samtalesimulatoren og adgangskontrollen og licensstyringen af kunderne. Derudover skal det vurderes, om behandlingen er proportional i forhold til at forfølge den legitime interesse. Dette skal også ske i lyset af det grundlæggende databeskyttelsesretlige princip om dataminimering, der følger af artikel 5, stk. 1, litra c.

### 3) Afvejning

**For det tredje** skal der foretages en afvejning ("balancing test"), hvor det skal vurderes, om de registreredes interesser eller grundlæggende rettigheder går forud for den dataansvarliges eller en tredjemands legitime interesse.

Den registreredes interesser og grundlæggende rettigheder kan navnlig gå forud for den dataansvarliges interesser, hvis personoplysningerne behandles under omstændigheder, hvor de registrerede, ikke med rimelighed kan forvente viderebehandling.[38]

Som nævnt ovenfor blev de enkelte behandlingsgrundlag kun berørt overfladisk og på et teoretisk plan, da projektet med samtalesimulatoren under sandkasseforløbet kun var i opstartsfasen.

Datatilsynet oplyste Børns Vilkår om, at kravene for anvendelsen af artikel 6, stk. 1, litra f som behandlingsgrundlag skal vurderes for hver enkelt behandlingsaktivitet: 1) Børns Vilkårs egen brug af samtalesimulatoren og 2) Børns Vilkårs anvendelse af personoplysninger i forbindelse med adgangskontrol og licensstyring. Dette gælder også for så vidt angår Børns Vilkårs brug af aggregeret data og KPI'er, hvis Børns Vilkår foretager en vurdering af om samme bestemmelse kan anvendes som behandlingsgrundlag for den behandlingsaktivitet.

Hvis Børns Vilkår baserer de ovenfor nævnte behandlingsaktiviteter på artikel 6, stk. 1, litra f, skal der i Børns Vilkårs videre arbejde med samtalesimulator-projektet foretages en afvejning af de registreredes og tredjeparters interesser eller grundlæggende rettigheder over for Børns Vilkårs legitime interesse i at behandle personoplysninger.

I den forbindelse skal følgende elementer identificeres og beskrives[39]:

1) De registreredes interesser, grundlæggende rettigheder og frihedsrettigheder[40]
2) Behandlingens påvirkning på de registrerede, herunder[41]
    a. typen af de personoplysninger, der skal behandles
    b. konteksten af behandlingen, og
    c. eventuelle yderligere konsekvenser af behandlingen
3) De registreredes rimelige forventninger[42]

[37] EDPBs udtalelse nr. 28/2024 om visse databeskyttelsesretlige aspekter relateret til behandlingen af personoplysninger i forbindelse med AI-modeller afsnit 3.3.2.2. og EDPBs vejledning nr. 1/2024 om behandling af personoplysninger baseret på artikel 6, stk. 1, litra f.
[38] Det følger af databeskyttelsesforordningens præambelbetragtning nr. 47.
[39] Elementerne er oplistet i pkt. 32 i EDPBs vejledning nr. 1/2024 om behandling af personoplysninger baseret på artikel 6, stk. 1, litra f.
[40] I EDPBs udtalelse nr. 28/2024 om visse databeskyttelsesretlige aspekter relateret til behandlingen af personoplysninger i forbindelse med AI-modeller pkt. 77.-81. er der beskrevet forskellige interesser og grundlæggende rettigheder, der kan være relevante at overveje i forbindelse med drift af en AI-model.
[41] De forskellige elementer i vurderingen af behandlingens påvirkning på de registrerede er nærmere beskrevet i EDPBs vejledning nr. 1/2024 om behandling af personoplysninger baseret på artikel 6, stk. 1, litra f pkt. 39.-49. og EDPBs udtalelse nr. 28/2024 om visse databeskyttelsesretlige aspekter relateret til behandlingen af personoplysninger i forbindelse med AI-modeller pkt. 82.-90.
[42] I EDPBs vejledning nr. 1/2024 om behandling af personoplysninger baseret på artikel 6, stk. 1, litra f, pkt. 54. fremgår en ikke-udtømmende liste over elementer, som kan indgå i vurderingen af de registreredes rimelige forventninger.

4) Den endelige afvejning af modstridende rettigheder og interesser, herunder muligheden for yderligere mitigerende foranstaltninger.[43]

## 3.5. Konsekvensanalyse

Databeskyttelsesforordningen kræver på flere punkter, at en dataansvarlig forholder sig til de risici en behandling af personoplysninger kan medføre for de registreredes rettigheder og frihedsrettigheder. Derudover skal den dataansvarlige kunne dokumentere de overvejelser og konklusioner, dette har givet anledning til.[44]

Personoplysninger skal behandles på en måde, der sikrer tilstrækkelig sikkerhed for de pågældende personoplysninger, herunder beskyttelse mod uautoriseret eller ulovlig behandling og mod hændeligt tab, tilintetgørelse eller beskadigelse. I den forbindelse skal der foretages en risikovurdering med henblik på at identificere de risici, der er forbundet med en behandling af personoplysninger og implementere foranstaltninger til at håndtere disse risici.[45]

Hvis behandlingsaktiviteten sandsynligvis vil indebære en høj risiko for fysiske personers rettigheder og frihedsrettigheder, skal Børns Vilkår desuden foretage en konsekvensanalyse.[46]

Datatilsynet og Børns Vilkår har drøftet overordnet, hvornår en dataansvarlig skal gennemføre en konsekvensanalyse. Datatilsynet har i den forbindelse oplyst, at det navnlig vil være relevant, hvis der ønskes anvendt ny teknologi. Det er Datatilsynets opfattelse, at det normalt vil være tilfældet ved udvikling og brug af AI-løsninger. Behandling af personoplysninger som led i drift af AI-løsninger vil ofte indebære en højere risiko for de personer, der behandles oplysninger om.

Børns Vilkår bør i den forbindelse få klarlagt:

- om der behandles personoplysninger ved brug af ny teknologi[47]
- om AI-løsningen i driftsfasen indebærer behandling af særlige kategorier af oplysninger, behandling af oplysninger om sårbare personer eller behandling af personoplysninger i stort omfang.

[43] I EDPBs udtalelse nr. 28/2024 om visse databeskyttelsesretlige aspekter relateret til behandlingen af personoplysninger i forbindelse med AI-modeller pkt. 99.-108. fremgår en ikke-udtømmende og ikke-bindende liste af foranstaltninger, der kan overvejes i forhold til drift af AI-modeller,
[44] Databeskyttelsesforordningens artikel 5, stk. 2, og artikel 24, stk. 1.
[45] Databeskyttelsesforordningens artikel 32 og artikel 5, stk. 1, litra f.
[46] Databeskyttelsesforordningens artikel 35, stk. 1.
[47] 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, s. 9. Det udgør også ét af kriterierne i Datatilsynets liste over de typer af behandlingsaktiviteter, der er underlagt kravet om konsekvensanalyse, jf. artikel 35, stk. 4, som er tilgængelig på tilsynets hjemmeside: Datatilsynets liste over de typer af behandlingsaktiviteter, der er underlagt kravet om en konsekvensanalyse.

Datatilsynet har henledt Børns Vilkårs opmærksomhed på, at det kun påhviler den dataansvarlige at foretage en konsekvensanalyse. Dette vil derfor betyde, at Børns Vilkår i de situationer, hvor Børns Vilkår er databehandler, ikke vil skulle tage stilling til, om der skal foretages en konsekvensanalyse. Det er derimod Børns Vilkårs kunder, der i de tilfælde skal foretage denne vurdering.

### Datatilsynets skabeloner til gennemførelse af konsekvensanalyse

Datatilsynet har udarbejdet to skabeloner til gennemførelse af konsekvensanalyser.

Den ene skabelon er af mere generisk karakter, og den anden skabelon vedrører specifikt konsekvensanalyse ved udvikling og drift af AI-løsninger.

I én af fanerne i skabelonerne er evalueringskriterierne for sandsynlighed og konsekvens beskrevet, ligesom at tilsynets risikomatrix er illustreret.

Her findes mere information om de to skabeloner:

- Nye skabeloner til gennemførelse af konsekvensanalyser.

# 4. Risikoklassificering efter AI-forordningen

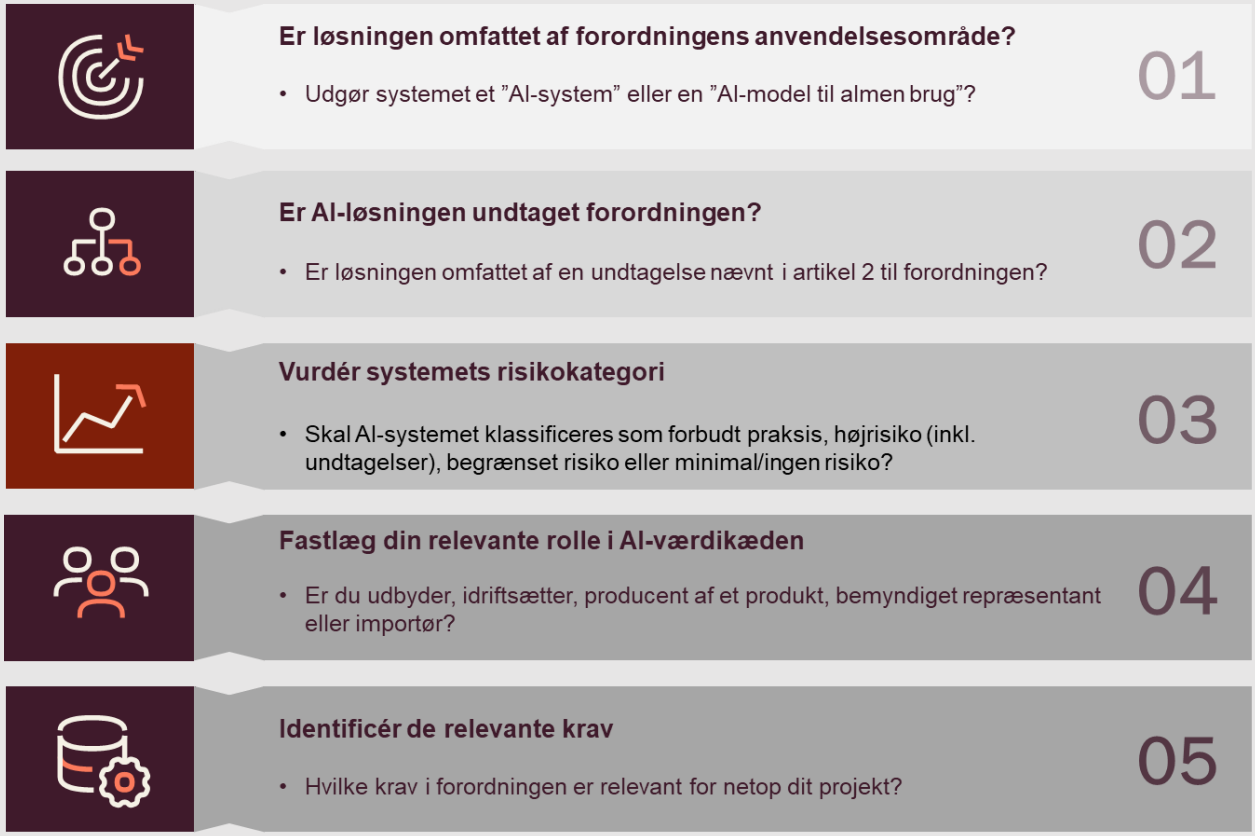
## 4.1. Indledning

AI-forordningen trådte i kraft den 1. august 2024 og har siden da løbende fundet anvendelse. Forordningen har på tidspunktet for udgivelsen af denne rapport ikke fået fuld virkning endnu. AI-forordningen fastsætter harmoniserede regler for omsætning, ibrugtagning og anvendelse af kunstig intelligens ("AI") i Den Europæiske Union. Formålet er bl.a. at fremme innovation og udbredelsen af AI og samtidig sikre et højt beskyttelsesniveau for sundhed, sikkerhed og de grundlæggende rettigheder i Unionen, herunder demokrati, retsstatsprincippet og miljøbeskyttelse, mod de skadelige virkninger af AI-systemer.

Med AI-forordningen er der etableret et nyt regelsæt, som griber direkte ind i måden, hvorpå AI-systemer udvikles og implementeres. AI-forordningen introducerer en række forpligtelser, som man med fordel kan arbejde med ud fra en struktureret metodisk tilgang, hvis de skal håndteres effektivt i praksis.

Dette arbejde må samtidig ske med bevidstheden om, at AI-forordningen er ny, og at en række bestemmelser, fortolkningsspørgsmål og grænsetilfælde endnu ikke er endeligt afklarede eller suppleret af relevante retningslinjer. Netop denne kompleksitet understreger betydningen af at arbejde tværfagligt i et AI-udviklingsprojekt. En tværfaglig tilgang styrker muligheden for tidligt i udviklingsprocessen at identificere regulatoriske udfordringer og træffe informerede beslutninger. Samtidig sikrer det, at man tager højde for reglerne fra begyndelsen - og ikke først bagefter.

Den regulatoriske vejledning om AI-forordningen har i AI-sandkassen været afgrænset til **risikoklassifikation** efter AI-forordningen. Forordningen introducerer en såkaldt **risikobaseret tilgang**, der indebærer, at typen og indholdet af reglerne er tilpasset graden og omfanget af de risici, som AI-systemer kan generere. En proces for risikoklassifikation kan illustreres på følgende vis:




Figur 2: Metodik for risikoklassificering

Det bemærkes, at processen ovenfor ikke nødvendigvis vil være den samme i alle AI-udviklingsprojekter, da behovet for afklaringer kan variere afhængigt af den konkrete situation. Processen er dog tænkt som en overordnet ramme, der kan bruges som udgangspunkt for arbejdet.

I det konkrete vejledningsprojekt med Børns Vilkår blev de fem trin i processen brugt til at skabe en ramme for de problemstillinger, der knytter sig til risikoklassificeringen. De efterfølgende afsnit følger derfor også de fem trin.

## 4.2. Trin 1) Er løsningen omfattet af AI-forordningen?

AI-forordningens artikel 2 fastlægger anvendelsesområdet og præciserer, hvilke aktører, systemer og aktiviteter AI-forordningen omfatter.

Det bør indledningsvist afklares, om ens løsning udgør et "AI-system" eller en "AI-model til almen brug" efter AI-forordningens definition heraf. AI-forordningens artikel 2 indebærer nemlig en **teknisk afgrænsning**. Et "AI-system" eller en "AI-model til almen brug" omfattes af forordningen, hvis det bringes i omsætning eller ibrugtages i EU, eller hvis systemernes output anvendes i EU.

AI-forordningen omfatter dermed ikke alle maskinbaserede teknologier. For Børns Vilkårs konkrete projekt var det relevant at vurdere, om der var tale om et "AI-system". I den sammenhæng har vejledningen kredset om definitionen af et AI-system i AI-forordningens artikel 3, stk. 1, nr. 1.

Definitionen af et "**AI-system**"[48] er kompleks og kan i praksis give anledning til fortolkningstvivl. En central egenskab ved AI-systemer er dog deres **evne til at udlede**. Denne evne til at udlede henviser til processen med at opnå output, f.eks. forudsigelser, indhold, anbefalinger eller beslutninger. Et andet centralt element i definitionen er, at AI-systemer er udformet til at fungere med varierende grader af autonomi. Det betyder, at de har en vis grad af **uafhængighed fra menneskelig medvirken** og har evnen til at fungere uden menneskelig indgriben.[49]

AI-forordningens anvendelsesområde er, foruden en teknisk afgrænsning til "AI-systemer" og "AI-modeller til almen brug", også afgrænset til en række bestemte kategorier af aktører. I AI-forordningen anvendes begrebet "operatør", som en samlebetegnelse for alle de aktører i AI-værdikæden, der er omfattet af AI-forordningen - på nær de berørte personer. De enkelte aktører behandles under afsnit 4.5.

Under vejledningsforløbet med Børns Vilkår opstod en central drøftelse af, hvordan man bør forstå begrebet "AI-system" efter forordningen. Drøftelsen drejede sig om, hvorvidt en samlet teknisk løsning kan anskues som **bestående af flere enkeltkomponenter**, hvor nogle indeholder AI, mens andre ikke gør. Det centrale spørgsmål var herefter, om hele den samlede løsning i sin helhed skal betragtes som et AI-system, eller om kun de komponenter i den samlede løsning, der faktisk indeholder AI, vil være omfattet af forordningen.

Drøftelsen tog konkret afsæt i spørgsmålet om, hvorvidt Børns Vilkårs samlede løsning, som beskrevet i afsnit 2.1, kunne anskues sådan, at dialogdelen via "barnebotten" ville indeholde AI, mens feedbackdelen via "coachbotten" (dvs. analysen af dialogen) ikke ville indeholde AI. Feedbackdelen via "coachbotten" skulle så anskues som bestående af en **deterministisk komponent**, der følger faste, menneskeskabte regler, uden egen læring eller inferens (dvs. uden at udlede nye resultater eller beslutninger på baggrund af input). En sådan komponent vil isoleret set typisk falde uden for definitionen af et AI-system. Anskuelsen ville også indebære, at alene en andel af den samlede løsning ville være omfattet af AI-forordningen.

En central læring i denne sammenhæng er, at vurderingen af, om et konkret softwaresystem falder ind under definitionen af et AI-system efter AI-forordningen, **ikke alene bør baseres på en isoleret og teknisk opdeling af løsningen i enkeltstående komponenter**. En funktionalitet, der kan kvalificeres som et selvstændigt element, og som i sig selv opererer helt uden for definitionen af et AI-system, vil som udgangspunkt ikke være omfattet af AI-forordningen. Indgår en sådan funktionalitet imidlertid som en integreret del af en samlet AI-løsning, der udfører inferens (udledning) og dermed opfylder definitionen af et AI-system, vil den i regulatorisk forstand kunne blive betragtet som en del af AI-systemet.

Dette bør ses i sammenhæng med, at EU-Kommissionens retningslinjer om definitionen af et AI-system lægger op til, at vurderingen af, om et softwaresystem udgør et AI-system, ikke begrænses til en isoleret teknisk analyse eller en mekanisk afkrydsningsøvelse. **Vurderingen bør i stedet**

[48] AI-forordningens artikel 3, stk. 1, nr. 1 og EU-Kommissionen retningslinjer for definition af AI-systemer.
[49] AI-forordningens præambelbetragtning nr. 12.

**baseres på systemets specifikke arkitektur og funktionalitet** samt tage hensyn til de syv elementer i definitionen af et AI-system.[50]

Med andre ord er det ikke kun relevant at se på, hvad et softwaresystem teknisk gør, og hvordan det teknisk er indrettet, men også at inddrage systemets **funktionalitet.** Det må også betyde, at vurderingen kan tage højde for, hvad systemet er tiltænkt at gøre, herunder skele til dets formål og tilsigtede anvendelse. Funktionalitet i den sammenhæng kan anses for at omfatte den samlede virkemåde og anvendelse af systemet, samt den tilsigtede anvendelseskontekst, hvori systemet indgår.

## 4.3. Trin 2) Er løsningen undtaget forordningen?

Da en eventuel undtagelse kan medføre, at forordningen ikke finder anvendelse på løsningen, vurderes undtagelserne forud for risikoklassifikationen og den nærmere fastlæggelse af de relevante roller i AI-værdikæden. Rollefastlæggelsen behandles derfor særskilt nedenfor under afsnit 4.5.

AI-forordningens artikel 2 indeholder en række udtrykkelige undtagelser fra forordningens anvendelsesområde. For alle AI-udviklingsprojekter er særligt undtagelsen om *videnskabelig forskning og udviklingsaktivitet* særlig relevant. Det skyldes, at reglerne i AI-forordningen ikke finder anvendelse på forsknings-, afprøvnings- eller udviklingsaktiviteter vedrørende AI-systemer, inden de bringes i omsætning eller ibrugtages.[51]

På tidspunktet for vejledningen i AI-sandkassen omfattede Børns Vilkårs projekt alene udviklingsaktiviteter. Udviklings- og afprøvningsaktiviteter kan under omstændighederne blandt andet omfatte udvikling og justering af modeller og algoritmer, træning og test på datasæt, validering af systemets ydeevne, fejlretning samt intern afprøvning i kontrollerede testmiljøer. Børns Vilkår vil først blive omfattet af kravene i AI-forordningen, når AI-systemet er bragt i omsætning.

## 4.4. Trin 3) Vurdér systemets risikokategori

Den risikobaserede tilgang i AI-forordningen udmøntes ved en inddeling i fire forskellige risikoniveauer:

| | |
|---|---|
| **Uacceptabel risiko:** | Otte bestemte former for AI-praksis vurderes efter AI-forordningens artikel 5 at udgøre en uacceptabel risiko, og disse former for AI-praksis kategoriseres derfor som forbudte inden for EU's grænser. |
| **Høj risiko:** | AI-systemer der klassificeres som højrisiko, kan medføre en væsentlig risiko for skade på sundheden, sikkerheden og borgernes grundlæggende rettigheder. Derfor er disse underlagt en række krav og forpligtelser for at nedbringe disse risici. |

[50] EU-Kommissionens retningslinjer for definition af et AI-system, betragtning 61.
[51] AI-forordningens artikel 2, stk. 8.

| | |
|---|---|
| **Begrænset risiko:** | Visse AI-systemer er underlagt gennemsigtighedsforpligtelser i henhold til AI-forordningens artikel 50, da de udgør en begrænset risiko for vildledning og misinformation. |
| **Minimal/ingen risiko:** | Forordningen stiller ingen krav til AI-systemer, der hverken indebærer uacceptabel, høj eller begrænset risiko. De indebærer dermed ingen eller alene en minimal risiko. Det kan for eksempel være AI i spamfiltre. |

I et AI-udviklingsprojekt kan det vise sig hensigtsmæssigt at starte med at kortlægge de forbudte former for AI-praksis, før man risikoklassificerer sit AI-system. På den måde kan man hurtigt sikre sig, at anvendelsen ikke indebærer en uacceptabel risiko. Derefter kan det vurderes, om brugen af systemet udgør en høj risiko, begrænset risiko eller en minimal risiko.

### 4.4.1. Trin 3.a) Forbudte former for AI-praksis

AI-forordningens artikel 5 indeholder et forbud mod otte nærmere angivne former for brug af et AI-system og mod at omsætte sådanne systemer. For en nærmere beskrivelse af de enkelte former for forbudt AI-praksis henvises der til EU-Kommissionen retningslinjer og Digitaliseringsstyrelsen nationale vejledninger.[52]

Børns Vilkårs løsning skal som beskrevet indgå som en del af et samlet forløb, hvor den fagprofessionelle trænes i Børns Vilkårs principper for samtaler med børn via en samtalesimulator. Træningen vil forventeligt indgå som led i et træningsforløb af medarbejdere på specifikke **arbejdspladser**, men kan også på sigt tænkes anvendt i **uddannelsessektoren** (nærmere herom i afsnit 4.4.2).

Af den grund har vejledningen i AI-sandkasseforløbet kredset om særligt det forbud, der følger af AI-forordningens artikel 5, stk. 1, litra f, hvorefter det inden for EU's grænser er **forbudt at bruge AI-systemer, der udleder følelser hos personer på arbejdspladser og uddannelsesinstitutioner**, undtagen hvis anvendelsen af AI-systemet er tilsigtet at blive bragt i omsætning af medicinske eller sikkerhedsmæssige årsager.

Grundlæggende indebærer forbuddet scenarier, hvor et AI-system anvendes til at analysere biometriske data, der stammer fra en person, f.eks. i form af stemmeleje, sprogbrug eller ansigtsudtryk, og med afsæt i disse biometriske data konkluderer/udleder, hvilken følelsesmæssig tilstand den pågældende person befinder sig i (f.eks. glad, sur, stresset, trist, begejstret). Begrebet "udlede" indebærer, at AI-systemer, som registrerer biometriske data om fysiske personer, skal udarbejde en form for konklusion på baggrund af registreringen. **Det er således afgørende**, at AI-systemet foretager en fortolkning/analyse af disse biometriske data. Det vil f.eks. indebære, at AI-systemet udleder, at når en fysisk person hæver stemmen, betyder det, at vedkommende er sur/vred.

Forbuddet indebærer også, at fysiske tilstande og synlige udtryk ikke vil være omfattet. Det gælder f.eks. panderynken, smil, eller systemer, der måler træthed. Et AI-system skal altså på baggrund af de synlige udtryk kunne udlede en reel følelse hos en person. Et eksempel på et scenarie, der henholdsvis er og ikke er omfattet, er følgende:

- AI-system konkluderer på baggrund af et smil, at en person er glad (omfattet)

[52] EU-Kommissionens retningslinjer om forbudte former AI-praksis og Digitaliseringsstyrelsen vejledninger herom.

- AI-system observerer, at en person smiler (ikke omfattet).

Vejledningen om Børns Vilkårs projekt har kredset om at sikre, at projektdeltagerne forstår de ovenfor anførte sondringer. Det er i den sammenhæng vigtigt at sikre, at AI-systemet ikke anvender biometriske data til at **udlede** den fagprofessionelles følelsesmæssige tilstand.

Hypotetisk kunne systemet via et kamera registrere, at den fagprofessionelles mundvige hælder nedad, og **på baggrund heraf udlede**, at den fagprofessionelle er vred, hvorefter feedbacken fra "coachbotten" ville antyde, at den fagprofessionelle burde smile mere under samtalen grundet den konstaterede følelsesmæssige tilstand. Selve konstateringen af et ansigtstræk vil ikke udgøre en forbudt AI-praksis. Hvis AI-systemet derimod *udleder* en følelse hos den ansatte baseret på sådanne biometriske data, vil dette kunne have karakter af en forbudt AI-praksis.

Vejledningen har desuden haft fokus på, at systemet ikke må foretage **indirekte udledninger** af følelser. Det vil sige, at feedback-delen i løsningen ikke bør drage konklusioner om den fagprofessionelles følelsesmæssige tilstand ud fra registreringer under dialogforløbet. Et eksempel på, hvad der bør undgås, er feedback, der udtrykker en følelsesmæssig vurdering, såsom: *"Barnet kan opfatte dig som sur på grund af dit toneleje"*.

Ovenstående illustrerer, hvordan tilføjelsen af en funktion i en løsning kan udgøre en forbudt AI-praksis. Derfor er det vigtigt, at udviklingsfasen foregår med kendskab til de forskellige former for forbudt praksis, så funktioner med tilhørende uacceptabel risiko ikke utilsigtet indarbejdes.

### 4.4.2. Trin 3.b) Højrisiko-AI-systemer

En central del af AI-forordningen omhandler reguleringen af højrisiko-AI-systemer. AI-systemer der klassificeres som højrisiko, kan medføre en væsentlig risiko for skade på sundheden, sikkerheden og borgernes grundlæggende rettigheder, men de er altså ikke forbudte. Højrisiko-AI-systemerne er dog underlagt en række krav i AI-forordningen, såsom detaljeret dokumentation, data- og risikostyring, overvågning og ansvarlighed. Formålet med kravene er at minimere den nævnte risiko.

I forhold til selve risikoklassifikationen følger det af AI-forordningens artikel 6, at et AI-system betragtes som højrisiko, hvis AI-systemet enten:

1) Er omfattet af de AI-systemer, der er oplistet i forordningens **bilag III**, eller

2) Tilsigtes anvendt som en sikkerhedskomponent i et produkt omfattet af nærmere angiven EU-produktsikkerhedsregulering eller selv er et produkt efter denne regulering (se forordningens **bilag I**).

Bilag III oplister otte områder og oplister for hvert område specifikke anvendelsestilfælde, som indebærer en høj risiko for skade på sundhed og sikkerhed eller for krænkelser af grundlæggende rettigheder. Overordnet set er områderne i bilag III oplistet som nummererede punkter, f.eks. punkt 1 (Biometri) og punkt 2 (Kritisk infrastruktur). De tilhørende anvendelsestilfælde er så anført under hvert enkelt område. Eksempelvis omfatter punkt 3 i bilag III området "uddannelse og erhvervsuddannelse", som indeholder tre anvendelsestilfælde (litra a–b).

For at et AI-system kan klassificeres som højrisiko efter bilag III, skal det altså være omfattet af et af områderne i bilag III og samtidig svare til et af de deri opregnede anvendelsestilfælde. Det følger heraf, at ikke alle AI-systemer, der anvendes inden for et givent område (såsom uddannelse og erhvervsuddannelse), automatisk anses for højrisikosystemer. Det er altså alene systemer, der falder inden for de specifikke anvendelsestilfælde, der er identificeret i bilag III, der er omfattet.

Risikoklassifikationen under AI-forordningen er **kontekstafhængig**, da det er løsningens konkrete anvendelse og **tilsigtede formål**, der afgør, om den falder under kategorierne i bilag III. Derfor kræves en systematisk screening af alle områder i bilaget for at identificere, hvor løsningen eventuelt "aktiverer" specifikke højrisiko-krav.

Vejledningsforløbet i AI-sandkassen har fokuseret specifikt på de højrisiko-områder, der grundet den tiltænkte anvendelse af løsningen kan være relevante for Børns Vilkår at være opmærksom på. Der er ikke foretaget en egentlig risikoklassificering af Børns Vilkårs projekt. Derimod er der under forløbet identificeret nogle højrisikoområder, baseret på løsningens tilsigtede formål og den konkrete anvendelseskontekst, som det er vigtigt at være opmærksom på.

Børns Vilkårs løsning vil som beskrevet forventeligt indgå som led i et træningsforløb af medarbejdere på relevante arbejdspladser, men kan også på sigt tænkes anvendt som træningsmateriale i uddannelsessektoren. På baggrund heraf har vejledningen i AI-sandkassen særligt kredset om højrisiko-områderne "Uddannelse og erhvervsuddannelse" og "Beskæftigelse" i bilag III, henholdsvis punkt 3 og 4.

Det følger af bilag III, punkt 3, at AI-systemer vil være højrisiko, hvis et AI-system inden for uddannelse og erhvervsuddannelsesområdet tilsigtes anvendt til at *"(...) evaluere læringsresultater, herunder når disse resultater anvendes til at styre fysiske personers læringsproces på uddannelsesinstitutioner på alle niveauer".* Bestemte systemer inden for uddannelsesområdet klassificeres som højrisiko-AI-systemer, da de kan afgøre en persons uddannelsesmæssige og arbejdsmæssige livsforløb og dermed påvirke denne persons mulighed for at sikre sig et livsgrundlag[53].

Hvis Børns Vilkårs AI-system implementeres i uddannelsesregi, kan det efter de konkrete omstændigheder udgøre et højrisiko-AI-system.[1] Det afgørende vurderingskriterium i den sammenhæng er, om AI-samtalesimulatoren konkret anvendes til at **evaluere læringsresultater** med henblik på at **styre** den studerendes videre læringsproces.

Dette kan f.eks. tænkes at være tilfældet, hvis løsningen indgår som en obligatorisk del af et uddannelsesforløb (f.eks. på socialrådgiveruddannelsen), og hvor resultaterne af den studerendes dialog med AI-samtalesimulatoren anvendes til at styre den videre læringsproces. Hvis fortsat deltagelse eller progression i et uddannelsesforløb gøres betinget af, at den studerende opnår en bestemt score, vurdering eller tilfredshedsgrad fastsat af AI-samtalesimulatoren, vil systemet i praksis fungere som en adgangs- eller selektionsmekanisme ("gatekeeper"). En sådan anvendelse, hvor AI-systemet foretager evaluering af læringsresultater og anvender disse til at styre den studerendes

[53] AI-forordningens præambelbetragtning nr. 56.

videre læringsproces, taler for, at AI-systemet i et sådant scenarie bør klassificeres som et højrisiko-AI-system i henhold til AI-forordningen.

Det vil være en helhedsorienteret vurdering af AI-systemet, om det er omfattet af et højrisiko-område. Det bør ske med udgangspunkt i **AI-systemets tilsigtede formål.** Herved forstås den specifikke sammenhæng og de specifikke betingelser for anvendelse som angivet i de oplysninger, udbyderen giver i brugsanvisningen, reklame eller salgsmaterialet og reklame- og salgserklæringerne samt i den tekniske dokumentation.[54]

Vurderingen bør således *ikke* være begrænset til en isoleret vurdering af enkelte komponenter i en samlet løsning. Hvis den samlede løsning er tiltænkt et anvendelsesformål omfattet af bilag III (højrisiko), vil AI-systemet som udgangspunkt blive klassificeret som højrisiko, medmindre en af de specifikke undtagelser i artikel 6, stk. 3, finder anvendelse.

Det følger også af bilag III, at AI-systemer vil være højrisiko, hvis AI-systemer tilsigtes anvendt *"(...) til at overvåge og evaluere personers præstationer og adfærd i sådanne forhold"* (arbejdsrelaterede kontraktforhold).[55] AI-systemer, der anvendes til at overvåge personers (ansattes) præstationer og adfærd, kan have en betydelig indvirkning på disse personers fremtidige karrieremuligheder, livsgrundlag og arbejdstagerrettigheder samt underminere deres grundlæggende ret til databeskyttelse og ret til privatlivets fred[56].

Hvis Børns Vilkårs AI-system implementeres på arbejdspladser, kan det efter de konkrete omstændigheder være et højrisiko-AI-system. Det afgørende vurderingskriterium i den sammenhæng er, om AI-samtalesimulatoren konkret anvendes til at "overvåge" og "evaluere" ansattes præstationer og adfærd.

Det kan f.eks. tænkes at indgå i vurderingen heraf, om der er tale om et isoleret læringsredskab til den enkelte medarbejder, hvor data/læringsresultater hverken logges eller videregives til ledelsen, eller om ledelsen derimod har indsigt i resultaterne. Det kunne også tænkes at være relevant at inddrage i vurderingen, om gennemførelse af dialogforløbet med AI-samtalesimulatoren med en bestemt score (fastsat af "coachbotten") er en forudsætning for fremtidige karrieremuligheder eller opgaveallokering på arbejdspladsen. I de tilfælde vil systemet reelt kunne fungere som et evalueringsværktøj af den ansattes adfærd og performance på det specifikke område.

Det er sandsynligt, at jo højere grad af ledelsesmæssig opfølgning og jo større indflydelse på den enkeltes progression eller ansættelsesforhold AI-systemet har, desto stærkere bliver formodningen for en højrisiko-kategorisering.

En anvendelse, hvor AI-systemet foretager evaluering og overvågning af læringsresultater fra dialogforløbet med en ledelsesmæssig opfølgning herpå, taler for, at AI-systemet i et sådant scenarie bør klassificeres som et højrisiko-AI-system i henhold til AI-forordningen, da dette konkret kan have en betydelig indvirkning på de ansattes fremtidige karrieremuligheder internt i virksomheden.

[54] AI-forordningens artikel 3, stk. 1, nr. 12.
[55] AI-forordningens bilag III, punkt 4, litra b ("beskæftigelse, forvaltning af arbejdstagere og adgang til selvstændig virksomhed").
[56] AI-forordningens præambelbetragtning nr. 57.

Hvis det konkrete AI-system vurderes ikke at være omfattet af hverken bilag III eller bilag I til AI-forordningen, vil AI-systemet enten være et AI-system med en begrænset risiko, eller et AI-system med en minimal/ingen risiko.

Det bemærkes, at det kan være relevant at overveje eller genbesøge ens risikoklassificering, når en ny version af AI-systemet rulles ud. Hvis systemets funktionalitet, formål eller andre væsentlige elementer ændres, kan det medføre, at systemet ved næste opdatering bliver omfattet af højrisikokravene eller andre relevante krav. Hvis et AI-system vurderes at være højrisiko efter AI-forordningens bilag III, bør man vurdere, om AI-systemet alligevel kan være undtaget efter en række foruddefinerede kriterier, der fremgår af AI-forordningens artikel 6, stk. 3. Betingelserne for disse undtagelser var i Børns Vilkårs tilfælde ikke umiddelbart opfyldt.

### 4.4.3. Trin 3.c) Begrænset risiko (Gennemsigtighedsforpligtelser)

Ifølge AI-forordningens artikel 50 gælder gennemsigtighedsforpligtelsen for visse AI-systemer, der er udviklet til at interagere med mennesker eller til at skabe indhold såsom billede, lyd, video og tekst. Disse systemer kan indebære særlige risici for misinformation eller vildledning, uanset om de er klassificeret som højrisiko eller ej.
Efter AI-forordningens artikel 50, stk. 1 skal udbydere af AI-systemer, der er tilsigtet at interagere direkte med fysiske personer, udformes og udvikles på en sådan måde, at de pågældende personer oplyses om, at de interagerer med et AI-system - medmindre det er indlysende.[57]

Til vurderingen af, om Børns Vilkår ved deres AI-system omfattes af forpligtelsen til at give oplysning efter artikel 50, stk. 1, kan det være relevant at inddrage forhold som f.eks. interaktionens karakter, anvendelsessammenhængen og graden af synlighed.
For Børns Vilkårs tilfælde taler de konkrete forhold for en oplysningsforpligtelse, idet brugerne/de fagprofessionelle gennem en brugergrænseflade kan interagere direkte med systemet via tale, og systemet vil svare med syntetisk tale. AI-systemet interagerer således direkte med personer.

Efter AI-forordningens artikel 50, stk. 2 skal udbydere af AI-systemer, der genererer syntetisk lyd-, billed-, video- eller tekstindhold, sikre, at AI-systemets output er mærket i et maskinlæsbart format og kan spores som kunstigt genereret eller manipuleret.

I vurderingen af, om kravet i artikel 50, stk. 2 finder anvendelse, er det relevant at se på, hvilket output løsningen genererer. I Børns Vilkårs konkrete case leverer AI-systemet feedback til brugeren om, hvordan dialogforløbet har været. Feedbacken produceres som syntetisk tekst, idet AI-systemet opsummerer og vurderer dialogen og genererer output baseret herpå. Derudover genereres syntetisk tale under brugerens interaktion med systemet. Disse forhold kan tale for, at løsningen omfattes af forpligtelsen til at mærke AI-systemets output i et *maskinlæsbart* format.

Når en større sprogmodel indarbejdes i en løsning som denne, kan det dog på nuværende tidspunkt, hvor de nærmere retningslinjer fra EU ikke er kommet, være vanskeligt at fastslå, *hvem* i den

[57] Om det er indlysende, vurderes ud fra *"en rimeligt velinformeret, opmærksom og forsigtig fysisk persons synspunkt ud fra omstændighederne og anvendelsessammenhængen"*.

samlede AI-værdikæde der skal foretage mærkningen af outputtet, herunder hvordan det konkret bør gøres.

Det fremgår af artikel 50, stk. 4, at *idriftsættere* af et AI-system, der genererer eller manipulerer billed-, lyd- eller videoindhold, der udgør en "deepfake", skal oplyse, at indholdet er blevet genereret kunstigt eller manipuleret.

Det er relevant for Børns Vilkår at være bekendt med kravene i artikel 50, stk. 4, i forbindelse med AI-samtalesimulatoren. Det skyldes, at den "avatar", som brugeren møder ved interaktion med AI-systemet, på sigt kan medføre, at idriftsættere af AI-systemet skal give oplysninger om, at indholdet er blevet genereret kunstigt eller manipuleret.

Dette vil forudsætte, at avataren udgør en "deepfake" efter AI-forordningens forstand. Det er konkret tilfældet, hvis AI genereret eller manipuleret billed- eller videoindhold, i **væsentlig grad ligner faktiske personer**, som fejlagtigt vil fremstå ægte eller sandfærdigt.[58] Det afgørende i den sammenhæng er derfor, om avataren i **væsentlig** grad ligner en **faktisk** person, eller om den er fuldstændig fiktiv. Det er hertil relevant at inddrage, i hvilken grad avataren efterligner udseende, stemme, mimik eller adfærd fra en faktisk person, så den kan fremstå ægte eller sandfærdig.

Baseret på den prototype af AI-systemet, som blev præsenteret under vejledningsforløbet, ligner avataren i sin nuværende version *ikke* i væsentlig grad en faktisk person, og vil i udgangspunktet ikke udgøre en "deepfake" efter AI-forordningen. Det er dog relevant for Børns Vilkår at være opmærksom på oplysningsforpligtelsen i artikel 50, stk. 4, da fremtidige ændringer i løsningen - eks. gennem opdateringer – på sigt kan gøre avataren mere realistisk og potentielt bringe den tættere på at udgøre en "deepfake" efter forordningens definition. Dette er særligt relevant, hvis avataren skabes ud fra en *faktisk* person.

EU-Kommissionen vil udgive retningslinjer om gennemsigtighedsforpligtelserne i artikel 50.

## 4.5. Trin 4) Fastlæg din relevante rolle i AI-værdikæden

AI-forordningens artikel 2 angiver en række aktører, som er tildelt forskellige krav og forpligtigelser alt efter, hvilken rolle de har i AI-værdikæden. I AI-forordningen anvendes begrebet "operatør", som en samlebetegnelse for alle de aktører i AI-værdikæden, der er omfattet af AI-forordningen, dog på nær de berørte personer.[59]

Forordningens to primære pligtsubjekter er imidlertid "udbydere" og "idriftsættere". En *udbyder* efter AI-forordningen er en fysisk eller juridisk person, en offentlig myndighed, et agentur eller et andet organ, der udvikler eller får udviklet et AI-system eller en AI-model til almen brug og bringer dem i omsætning eller ibrugtager AI-systemet under eget navn eller varemærke, enten mod betaling eller gratis.[60] En *idriftsætter* efter AI-forordningen er en fysisk eller juridisk person, en offentlig myndighed,

[58] Relevante dele af definitionen af en "deepfake" efter AI-forordningens artikel 3, stk. 1, nr. 60.
[59] AI-forordningens artikel 3, stk. 1, nr. 8.
[60] AI-forordningens artikel 3, stk. 1, nr. 3.

et agentur eller et andet organ, der anvender et AI-system under sin myndighed, medmindre AI-systemet anvendes som led i en personlig ikkeerhvervsmæssig aktivitet.[61]

Under vejledningen i AI-sandkassen er det identificeret, at der kan opstå vanskelige grænsetilfælde, når en leverandør udvikler et AI-system til en "kunde" (her Børns Vilkår), og hvor der sker tilpasninger af et eksisterende system. I disse situationer efterlader AI-forordningen tvivl om rækkevidden af begrebet "udbyder". Særligt relevant under drøftelserne i vejledningsforløbet var sammenhængen mellem det at "få udviklet et AI-system" og den rolle, man indtager som "udbyder".

I vurderingen af Børns Vilkårs rolle i AI-værdikæden vil der kunne indgå en række momenter, herunder at Børns Vilkår foranlediger tilpasninger af et eksisterende AI-system fra en leverandør til egne, specifikke behov, herunder ændringer i anvendelsesformål, prompting eller anvendelse af egne datasæt, særligt da sådanne tilpasninger kan have betydning for systemets adfærd eller risikoprofil. Børns Vilkår tilkendegav under vejledningsforløbet, at de påtænker at prompte AI-samtalesimulatoren (hhv. "barnebotten" og "coachbotten") med bl.a. undervisningsmateriale og fiktive cases, som Børns Vilkår selv ville udarbejde. I forlængelse heraf blev det oplyst, at leverandøren i starten ville assistere Børns Vilkår med at prompte simulatoren, men at Børns Vilkår på sigt selv ville prompte simulatormodellen uden leverandørens deltagelse. Desuden kan det indgå som et moment, at Børns Vilkår har tilkendegivet et ønske om at ibrugtage og udbyde systemet under eget navn, logo eller varemærke, hvormed de udadtil fremstå som ansvarlig for løsningen over for brugerne.

På baggrund af de konkrete forhold - særligt at Børns Vilkår **tilpasser og får udviklet AI-systemet til et specifikt formål**, **overtager prompt-styringen**, og vil **markedsføre løsningen under sit eget navn og logo** - bør Børns Vilkår betragtes som udbyder efter AI-forordningen. En endelig vurdering skal naturligvis stadig tage udgangspunkt i de specifikke forhold i den enkelte sag, men de nævnte elementer taler tydeligt i retning af udbyderstatus.

## 4.6. Trin 5) Identificér de relevante krav

Når risikoen ved AI-systemet og organisationens rolle i AI-værdikæden er afklaret, er næste skridt at orientere sig i de relevante krav i AI-forordningen. Hvilke forpligtelser der gælder, afhænger både af systemets risikoniveau og af organisationens rolle i relation til systemet. *Udbydere* af højrisiko-AI-systemer skal f.eks. etablere et risikostyringssystem, sikre korrekt datastyring og udarbejde teknisk dokumentation. *Idriftsættere* af højrisiko-AI-systemer skal blandt andet følge den brugsanvisning, som udbyderen udarbejder, og sikre, at menneskeligt tilsyn varetages af personer med de nødvendige kompetencer.[62] Hertil kommer, at alle organisationer, der udbyder og idriftsætter AI-løsninger, skal sikre, at deres medarbejdere besidder tilstrækkelige AI-færdigheder. Læs mere herom i Digitaliseringsstyrelsens vejledning AI-færdigheder.[63]

[61] AI-forordningens artikel 3, stk. 1, nr. 4.
[62] Se hertil AI-forordningens artikel 9-22 (krav til udbydere) og art. 26 (krav til idriftsættere).
[63] Digitaliseringsstyrelsens vejledning om AI-færdigheder.

# 5. Vejen frem

Børns Vilkårs indsats i sandkasseforløbet har været kendetegnet ved åbenhed, fleksibilitet og en stræben efter at efterleve de regulatoriske krav i alle henseender – herunder i tvivlstilfælde. Børns Vilkår har mellem møderne i sandkasseforløbet og på baggrund af drøftelserne i projektet uddybet deres overvejelser og spørgsmål samt udfærdiget supplerende materiale i forhold til de påtænkte behandlingsaktiviteter forbundet med løsningen, datastrømmene mellem de involverede aktører og de forskellige roller, Børns Vilkår har i forhold til henholdsvis kunder og systemleverandør.

For at sikre at udviklingen af AI-løsningen sker i overensstemmelse med databeskyttelsesreglerne, er det Datatilsynets og Digitaliseringsstyrelsens forventning, at Børns Vilkår efter sandkasseforløbets afslutning arbejder videre med særligt vurderingerne om rolle- og ansvarsfordeling og brugen af aggregerede og anonymiseret data.

I forhold til AI-forordningen skal Børns Vilkår desuden arbejde videre med den egentlige risikoklassificering og den samlede tilrettelæggelse af regelefterlevelsen af AI-forordningen i tæt samarbejde med den valgte leverandør. Børns Vilkår skal herudover løbende følge udviklingen i det regulatoriske grundlag. Det indebærer at holde sig orienteret i kommende retningslinjer fra EU-Kommissionen, nationale vejledninger fra Digitaliseringsstyrelsen og harmoniserede standarder.

Det er også relevant at holde sig orienteret om eventuelle justeringer til AI-forordningen som følge af forslaget om den digitale omnibus til AI-forordningen, der kan få betydning for både krav og tidsmæssig anvendelse.

Datatilsynet og Digitaliseringsstyrelsen har i sandkasseforløbet fået et indblik i de forskellige rollekonstellationer ved udviklingen og idriftsættelsen af AI-løsningen, hvor der er flere aktører involveret, og hvor disse har forskellige ansvarsområder.

Datatilsynet og Digitaliseringsstyrelsen vil inddrage disse aspekter i deres vejledningsarbejde for på den måde at bidrage til, at eventuelle uklarheder i forhold til de databeskyttelsesretlige og AI-retlige problemstillinger ikke står i vejen for brugen af AI til innovations- og effektiviseringstiltag.

*"I Børns Vilkår har vi været utroligt glade for den meget konkrete sparring vi har fået. Vi har stået med et nyt og komplekst produkt, som skulle matches ind i et nyt og komplekst lovområde.*

*Her har vi oplevet Digitaliseringsstyrelsen og Datatilsynet som meget konstruktive og praksisnære i deres tilgang, og det har givet os mulighed for at tilpasse løsningen i takt med projektets udvikling. Det har været værdifuldt at integrere begge myndigheders kompetencer. De har sat sig grundigt ind i vores specifikke løsning samt vores ideer for at diskutere, hvordan lovgivningen skulle fortolkes med de forskellige alternativer.*

*Diskussionerne har medført ændringer i vores tekniske løsning, i vores kommunikation med leverandøren samt i en udbygning af vores kvalitetssystem, så det understøtter de regulatoriske krav, AI-forordningen stiller til vores system.*

*Det ville have været en fordel, hvis vores AI-projekt havde været lidt længere fremme i udviklingsfasen, så der havde været bedre mulighed for at inddrage opdateret viden om AI-løsningens tekniske set-up og dermed sikre mere målrettet vejledning fra myndighedernes side"*

- **Børns Vilkår.**

DATATILSYNET

Digitaliserings-
styrelsen