# Konsekvensanalyse

Signaturprojekt ”AI beslutningsstøtte til behandling af kommunale aktindsigtssager og open source-udstilling af kommunale sprogmodeller”


Et tværkommunalt samarbejde

Vejen KOMMUNE

FREDENSBORG KOMMUNE

Sønderborg

| | |
|---|---|
| Dataansvarlig: | |
| Udfyldt af: | Projektsekretariatet AI aktindsigt |
| Ansvarlig kontaktperson: | Katharina Stengaard; Jesper Schmidt |
| Repræsentant for ledelsen: | |
| Databeskyttelsesrådgiver: | |
| System(er) der anvendes til projektet: | |

## Versionsstyring

| Version, dato | Bemærkninger |
|---|---|
| V.1, *07. marts 2022* | Udarbejdelse af første version af konsekvensanalysen |
| V.2, 02. december 2022 | *Udkast til ledelsesgodkendelse* |
| V.3, 02. maj 2023 | Endelig version til offentliggørelse |

# Indhold

# Sammenfatning

Konsekvensanalysen kan overordnet sammenfattes på følgende måde:

Det vurderes, at denne DPIA kan godkendes af ledelsen.

Denne konsekvensanalyse er lavet på Signaturprojektet "AI beslutningsstøtte til behandling af kommunale aktindsigtssager og open source-udstilling af kommunale sprogmodeller". Forud for eventuel overgang til drift skal konsekvensanalysen revurderes med henblik på at genvurdere risici og mitigerende foranstaltninger i forbindelse med et driftsscenarie.

Databeskyttelsesrådgiveren har været inddraget i udarbejdelsen af DPIA (og projektet generelt) i udvidet grad. Datatilsynet samt Kammeradvokaten er blevet hørt inden idriftsættelse og deres anbefalinger er blevet efterkommet.

Konsekvensanalysen påtænkes offentliggjort på projekthjemmeside.

# Indledning og baggrund

## Konsekvensanalysens formål

Formålet med denne konsekvensanalyse vedrørende databeskyttelse er at beskrive den behandling af personoplysninger, som Sønderborg Kommune, Vejen Kommune og Fredensborg Kommune vil foretage i forbindelse med udvikling samt anvendelse af sprogmodeller (Natural Language Procesing (NLP)) til beslutningsstøtte i arbejdet med Aktindsigter. NLP-modellerne udvikles som del af et Signaturprojekt "AI beslutningsstøtte til behandling af kommunale aktindsigtssager og Open Source-udstilling af kommunale sprogmodeller".

Vurderingerne foretaget i DPIA'en er begrænset til projektperioden. Ved eventuel overgang til drift skal DPIA'en genevalueres og tilpasses hvor relevant.

I behandling af aktindsigter gennemføres en række aktiviteter, som beskrevet i figur 1. Projektet omhandler den specifikke og afgrænsede aktivitet 3: "Relevante dokumenter gennemgås for informationer som potentielt skal udelades". Denne DPIA samt de vurderinger der er foretaget i forbindelse med udarbejdelse af denne er ligeledes afgrænset til at omhandle aktivitet 3.

*Figur 1: Behandlingsaktiviteter i forbindelse med behandling af aktindsigt*


I projektet deltager foruden de tre ovennævnte kommuner også databehandleren Aktio samt underdatabehandler Alvenir. De tre kommuner er selvstændigt dataansvarlige for egne data, og har hver især særskilte databehandleraftaler. De data, den enkelte kommune bidrager med til træning og udvikling af modellerne, forlader ikke den enkelte kommunes IT-miljø, og kommunerne får ikke adgang til hinandens data.

Konsekvensanalysen har endvidere til formål at afdække risici forbundet med behandlingen af personoplysninger i AI-løsningen samt bidrage til at håndtere disse risici for fysiske personers rettigheder og frihedsrettigheder ved at vurdere dem og fastlægge foranstaltninger til at afhjælpe dem.

Denne konsekvensanalyse er udarbejdet i overensstemmelse med minimumskravene til en konsekvensanalyses indhold i databeskyttelsesforordningens artikel 35, stk. 7, samt i bilag 2 til Artikel 29-Gruppens (nu: Det Europæiske Databeskyttelsesråd) vejledning om konsekvensanalyser.[1]

Konsekvensanalysen skal således bidrage til at sikre overholdelse af databeskyttelsesforordningens og databeskyttelseslovens regler, ligesom den er en væsentlig forudsætning for overholdelse af forordningens grundlæggende princip om ansvarlighed – dvs. dokumentation for overholdelse af forordningens regler, jf. forordningens artikel 5, stk. 2, og artikel 24. En konsekvensanalyse har endvidere en naturlig sammenhæng til reglerne om indbygget databeskyttelse (privacy by design) derved, at en konsekvensanalyse kan give værdifuldt input til kravsætning til databeskyttelsen i løsningsdesignet.

## Baggrunden for konsekvensanalysen

Årsagen til udarbejdelsen af denne konsekvensanalyse er følgende:

Databeskyttelsesrådgiveren har anbefalet, at Sønderborg Kommune som dataansvarlig foretager en konsekvensanalyse af AI-løsningen med udgangspunkt i projektbeskrivelsen.

Vurderingen er baseret på, at AI-Signaturprojektet indebærer udvikling af sprogmodeller, der skal yde beslutningsstøtte i arbejdet med aktindsigtssager, som omfatter en stor mængde personoplysninger henhørende både almindelige og særlige kategorier af personoplysninger, hvilket indebærer en høj risiko for registreredes rettigheder og frihedsrettigheder, jf. databeskyttelsesforordningens artikel 35, stk. 1.

Konsekvensanalysen gennemføres derudover for at sikre, at eventuelle tilkommende tekniske eller organisatoriske krav/løsninger vil blive belyst og implementeret under hensyn til databeskyttelsen.

# Trin 1: Systematisk beskrivelse af behandlingen af personoplysninger i AI-løsningen

## AI-løsningens formål og karakter

Formålet med behandlingen af personoplysninger i AI-løsningen er følgende:

Formålet med løsningen er at fremsøge og identificere oplysninger i sagsakter, som potentielt indeholder oplysninger der skal overstreges i en aktindsigt inden den sendes til anmoder i henhold til gældende lovgivning. Det kan for eksempel være oplysninger så som CPR-nummer på anden person end modtager eller en adresse på en borger med hemmelig adresse.

[1] Artikel 29-Gruppen (nu Det Europæiske Databeskyttelsesråd, herefter forkortet "EDPB"): Retningslinjer for konsekvensanalyse vedrørende databeskyttelse (DPIA) og bestemmelse af, om behandlingen "sandsynligvis indebærer en høj risiko" i henhold til forordning (EU) 2016/679, WP 248, rev. 01, revideret og endeligt vedtaget den 4. oktober 2017

Arbejdet med ovenstående forløber i to overordnet faser:

1. Først handler det om at udviklet et sæt af AI sprogmodeller, der kan assistere sagsbehandlere i behandlingen af Aktindsigtssager.
2. Sprogmodellerne kan ikke stå alene, og sættes i produktion til behandlingen af aktindsigt ved at være en integreret del af IT-løsningen Aktio Indsigt, som allerede anvendes i Sønderborg Kommune.

Begge emner vil løbende blive behandlet i denne DPIA. Når de udviklede AI sprogmodeller sættes i produktion i IT-løsningen Aktio Indsigt, vil der være tale om et sagsbehandlingssystem til aktindsigt som anvender AI til at effektivisere arbejdsproces og opgaveløsning i behandlingen af aktindsigtsager.

Udviklingen af AI sprogmodeller har fokus på to typer af modeller.

1. NER-model: denne model trænes i at fremsøge specifikke entiteter (ord eller talrækker) som potentielt skal udelades. Det kan for eksempel være CPR-numre, navne, adresser eller diagnoser.
2. Semantisk søgemodel: denne model søger efter sammenhænge og relationer i større tekstmængder. Dette kan blandt andet bruges til at fremsøge relevant dokumenter, eller identificere dokumenter der skal udelades (fx interne arbejdsdokumenter).

De udviklede sprogmodeller vil blive anvendt som beslutningsstøtte til sagsbehandleren som træffer de afgørende beslutninger i en sag. Fx vil en sprogmodel effektivt kunne identificere repræsentationen af fx navne på tværs af 1000 dokumenter, og foreslå at disse ekstraheres pga. GDPR lovgivning, men det er sagsbehandleren som træffer afgørelsen om at det forholder sig sådan.

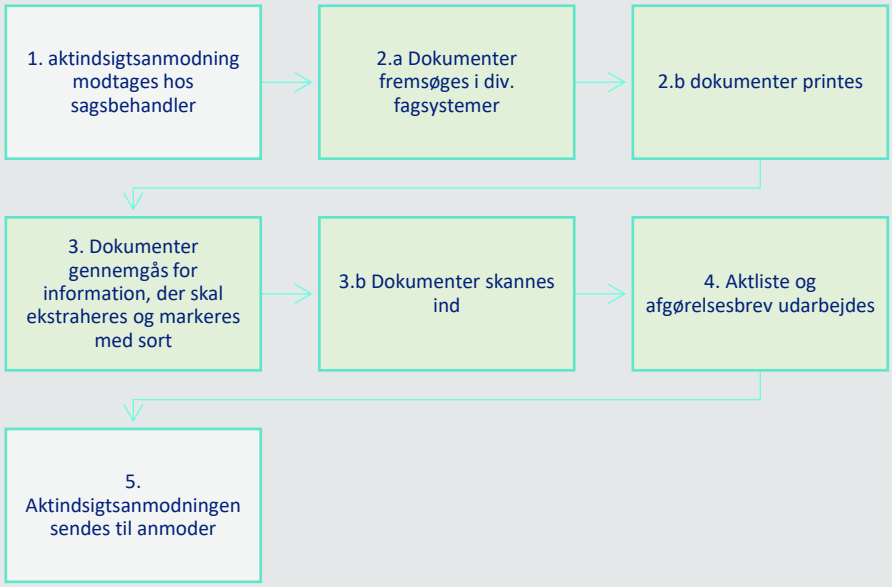
Jf. Offentlighedsloven §7 og Forvaltningsloven §9 har enhver borger ret til at anmode om aktindsigt. Regler for udeladelse af informationer i aktindsigter fremgår blandt andet af Offentlighedsloven kapitel 4 §§19-35, Forvaltningsloven og Retsplejeloven. Retten til aktindsigt fremgår ligeledes af Miljøoplysningsloven og Sundhedsloven.

Intentionen med AI løsningen er at effektivisere en proces, som kommunen er forpligtet til at gennemføre, jf. ovenstående. Ved at anvende sprogmodeller til beslutningsstøtte i forbindelse med behandling af aktindsigt er forventningen at kunne forkorte sagsbehandlingstiden for de registrerede, samt mindske ressourceforbruget for kommunen. Det forventes også, at løsningen er med til at kvalitetssikre arbejdet med aktindsigter, og dermed reducere antallet af anmeldelser om sikkerhedsbrud.

Karakteren af behandlingen af personoplysninger i AI-løsningen kan beskrives på følgende vis:

Arbejdet med aktindsigter er omfattende og ressourcekrævende. Arbejdet er i dag præget af en række manuelle processer, som er tidskrævende for sagsbehandler. Processen for behandlingen varierer fra afdeling til afdeling, men i hovedtræk foregår det således:

*Figur 2: Manuel proces for behandling af aktindsigt*




Dele af denne manuelle proces kan automatiseres fx ved en digital platform til behandling af dokumenter samt RPA til indsamling af dokumenter.

De sprogmodeller, som udvikles og sættes i produktion under dette projekt, vil i særdeleshed understøtte trin 3 ”Dokumenter gennemgås for information, der skal ekstraheres”. De trænede NLP sprogmodeller vil blive integreret i en IT-løsning med en brugerflade (GUI), hvorfra en sagsbehandler kan ‘aktivere’ modellerne til at assistere med at scanne dokumenter for fx personfølsomme informationer. Den ene type trænet sprogmodel (NER-model) bliver trænet til at identificere disse informationer i en tekst, og i samspil med IT-løsningens brugerflade stilles der forslag til sagsbehandler om at ekstrahere og mørklægge fx personfølsomme informationer.

Det vurderes, at brugen af en beslutningsunderstøttende AI løsninger kan mindske ressourcetrækket samt kvalitetssikre og strømline behandlingen af aktindsigter.

Intentionen er at udvikle to typer sprogmodeller (NER-model og semantisk søgning), som trænes med machine learning. Der udpeges specifikke entiteter (32+) som NER-modellen trænes i at fremsøge. Begge modeller understøttes af regelbaseret teknologi.

Modellerne har ikke en direkte indflydelse på de registrerede, da de udelukkende er understøttende af allerede eksisterende arbejdsgange. Formålet med AI-løsningen er netop at optimere denne arbejdsgang, ved at hjælpe sagsbehandler med at fremsøge informationer, som de ellers manuelt skulle fremsøge (figur 2). AI løsningen anvendes dermed i behandlingsfasen af aktindsigtsprocessen (figur 3).

Da løsningen udvikles til understøttelse af dokumentfremsøgning samt gennemgang af dokumenter ved en aktindsigtsanmodning vil sagsbehandler løbende gennem behandlingen blive anmodet om at tage aktiv stilling til de elementer, som fremsøges. Hertil kommer, at sagsbehandler forholder sig til

databeskyttelsesretlige forhold, herunder men ikke afgrænset til principperne om formål, dataminimering samt de registreredes rettighede.

Det vil for eksempel være sagsbehandler der definerer, med hvilken lovhjemmel information ekstraheres. Dermed skal forstås, at sagsbehandleren forholder sig til aktindsigtsanmodningens karakter i forhold til den information, som kan fremsøges.

I henhold til lovgivningen for aktindsigt skal det vurderes hvilke dokumenter, der udleveres ved en aktindsigtsanmodning. Det vil således være sagsbehandlers ansvar at gennemgå aktindsigten og aktlisten inden denne sendes ud.

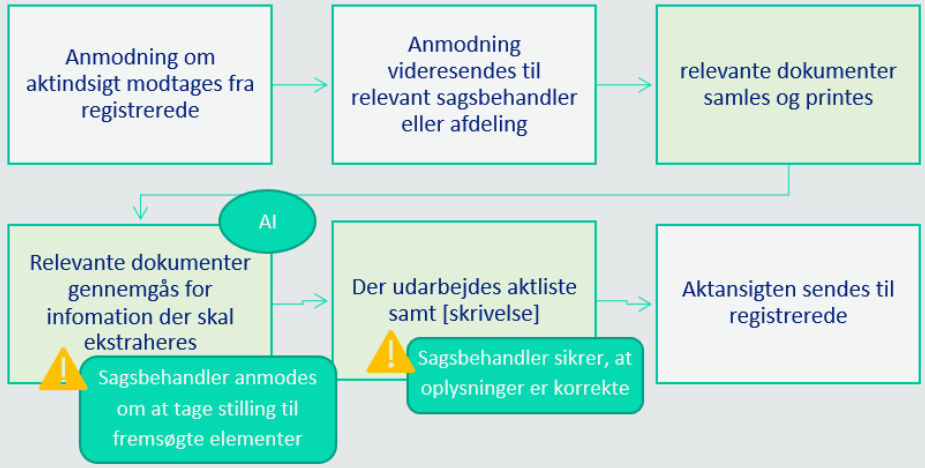
Den færdigtrænede NER-model forventes at have en præcision i prædiktion af informationer i tekst >90%. Hvilket vil sige at i mere end 9/10 sammenhæng, hvor den fx skal identificere en personfølsom information som diagnoser, da vil NER-modellen kunne identificere repræsentationen (variation af forskellige diagnoser og gentagelser) af diagnoser på et splitsekund.

Træningen af de modeller som udvikles og sættes i drift vil forløbe i iterationer, hvor modeller hele tiden justeres, inden den igen sættes i træning på en ny mængde data. Sådan vil modellen hele tiden blive videretrænet indtil den opnår det højst muligt performancemål >90%. Som kontrol bliver 20% af den oprindelige data anvendt til kontroltest, som skal bevise den endelige NER-models performance. Dvs. 'fremmede' data af samme kvalitet som den data modellen er trænet på, og som ikke er anvendt til træning bruges til at måle og dokumentere NER-modellens performancescore.

I forbindelse med indsamling af data har datatilsynet godkendt, at tidligere behandlet aktindsigtssager anvendes som data til træning af NER-model. Disse data vil indgå i puljen af samlet data, som NER-modellen trænes på.

I forbindelse med en senere drift af en NER-model skal det bemærkes, at en NER-model ikke i sig selv træffer afgørelse i aktindsigtssager, men alene har den kvalitet at den effektivt kan scanne dokumenter for fx personfølsomme og/eller personhenførbare oplysninger. Det vil fortsat være de enkelte sagsbehandlere som behandler og træffer afgørelse i sager om aktindsigt. En NER-model kan ikke træffe afgørelser, endsige medvirke til forskelsbehandling i de afgørelser som træffes i aktindsigtssager.

Figur 3: Proces for udarbejdelse af aktindsigt




# AI-løsningens behandling af personoplysninger og omfanget heraf

AI-løsningen medfører behandling af følgende personoplysninger på følgende måder:

Retten til aktindsigt dækker alle områder, hvor oplysninger om borgere (og virksomheder) behandles. Derfor vil løsningen behandle alle typer personoplysninger der kan indgå i et kommunalt dokument, som behandles ifm. AI-løsningens screening til brug for ekstrahering under aktindsigtsprocessen. Dermed behandles almindelige personoplysninger (ikke-følsomme oplysninger), særlige kategorier af personoplysninger (følsomme oplysninger) samt oplysninger om straffedomme og lovovertrædelser eller tilknyttede sikkerhedsforanstaltninger i løsningen. Hertil kommer fortrolige oplysninger (ofte underlagt særregulering i anden lovgivning)). Alle oplysninger anvendes nødvendigvis i træning, test og anvendelse af modellerne. Dette da modellen ikke kan "lære" at genkende for eksempel helbredsoplysninger, hvis ikke den har haft mulighed for at træne på data hvor dette fremgår. Ligeledes kan effektiviteten af modellerne ikke bevises, hvis ikke oplysningerne anvendes til validering af modellerne. Oplysninger der anvendes i træningen, vil være pseudonymiserede.

Efter sagsbehandlingen af aktindsigten er afsluttet, benyttes data til forbedring af de to sprogmodeller, som indgår i AI løsningen.

Sprogmodellerne trænes på et datasæt som indeholder persondata, hvilket er en absolut nødvendighed for at kunne opnå en høj performance for især en NER-model. Differential privacy som anvendes i træningen af modeller sikrer, at ingen data med personoplysninger kan udledes fra den færdigtrænede model. Ligeledes forholder det sig med test af modellens performance, som nødvendigvis skal ske på tilsvarende data for at kunne validere modellens performancescore, og præcisionen i at kunne identificere emner, som den er trænet til at identificere fx navne.

I træningen af en NER-model fremtrænes modellens egenskaber på baggrund af 80% af den totale mængde data. De resterende 20% af det samlet datasæt tilbageholdes og anvendes til at teste modellen performance. Således anvendes de resterende 20% som benchmark og validering af modellens egenskab til, fx at identificere navne, diagnoser, m.m. i tekst som den er trænet til at identificere.

Aktio-indsigt er installeret på lokale servere internt i kommunerne, hvorpå data brugt til behandling af aktindsigter opbevares. Træning af sprogmodellerne foregår på en separat GPU. Efter overførsel og træning i den enkelte kommune slettes disse data fra GPU'en.
Da der er tale om en digital platform vil der ikke være behov for at printe data til papirformat i selve behandlingen af aktindsigten.

Omfanget af AI-løsningens behandling af personoplysninger kan beskrives på følgende vis:

**Det skal her bemærkes, at AI løsningen understøtter en eksisterende arbejdsgang. Den her beskrevne behandlingsaktivitet er derfor uafhængig af AI-løsningen, og vil gennemføres uagtet om AI løsningen er i anvendelse eller ej.**

Jf. offentlighedsloven §7 kan " […] Enhver forlange at blive gjort bekendt med dokumenter, der er indgået til eller oprettet af en myndighed m.v. som led i administrativ sagsbehandling i forbindelse med dens virksomhed.". Dermed kan anmoder for eksempel være:

- Borgere, der ønsker indsigt i egen sag
- Pårørende der søger indsigt i en andens sag
- Forældre der søger indsigt i barnets sag
- En borgers stedfortræder (fx advokat)
- Anden myndighed der søger aktindsigt i en borgersag (fx i forbindelse med tilflytning)
- Virksomheder fx i forbindelse med Udbud (ikke personoplysninger)
- Journalister

Den registrerede vil i behandlingen af en aktindsigtssag være den person (ved borgersager) som aktindsigten omhandler, og altså ikke anmoder. Registrerede kan, ved borgersager, være enhver borger.

Der føres ikke statistik over antallet af aktindsigtsanmodninger, hvorfor der ikke er et præcist antal af registrerede hvis oplysninger behandles. Det vurderes at der i gennemsnit er 1.000-1.200 aktindsigter årligt i Sønderborg Kommune.

Der er store forskelle i størrelsen på en aktindsigtsanmodning både i forhold til mængden af dokumenter og indholdet af personoplysninger. For eksempel kan en børnesag indeholde op mod 300 dokumenter indeholdende en større mængde fortrolige oplysninger om fx helbred. Til sammenligning kan en aktindsigt i forbindelse med en klagesag indeholde få dokumenter med en begrænset mængde personoplysninger. I sagens natur, vil oplysningerne være personhenførbare.

Informationer, som omhandler anden person end den registrerede (personen aktindsigten omhandler) skal oftest ekstraheres, inden aktindsigten fremsendes. Derfor vil der, i behandlingen af aktindsigten også være personhenførbare personoplysninger (fx navn, CPR-nr.) på andre registrerede end den, aktindsigten omhandler.
I visse afdelinger er der op til flere aktindsigtsanmodninger om ugen, hvorfor behandlingen med understøttelse af AI løsningen vil være kontinuerlig.
Dokumenterne der anvendes i AI løsningen er opbevaret på kommunernes egne servere (Sønderborg Kommune, Vejen Kommune eller Fredensborg Kommune). Oplysningerne forlader ikke kommunen, hverken i forbindelse med behandling af aktindsigten eller træning af modellerne. Træningsdata blandes ikke tværkommunalt, og hver kommune har alene adgang til de personoplysninger, de selv er dataansvarlige for. Den udarbejdede aktindsigt sendes med sikker post til anmoder, hvormed oplysningerne trækkes ud af kommunernes lokale miljøer. Herefter overgår dataansvar til anmoder.

## Sammenhæng og kontekst for behandlingen af personoplysninger i AI-løsningen

Den sammenhæng og kontekst, som behandlingen af personoplysninger i AI-løsningen indgår i, kan beskrives på følgende vis:

Da arbejdsgangen allerede er eksisterende, har dataansvarlig på forhånd erfaring med behandlingsaktiviteten. Dataansvarlig (kommunen) behandler registreredes oplysning efter anmodning fra registrerede eller dennes pårørende, myndige eller stedfortræder (fx advokat). Dermed kan anmoder i princippet være alle, herunder også børn eller andre sårbare grupper.

Kommer anmodning fra anden myndighed (fx tilflytterkommune), vil der være tale om en partshøring og ikke en aktindsigt.

Oplysningerne i en aktindsigtssag er på forhånd eksisterende oplysninger, og opbevares under relevant lovgivning herunder i henhold til registreredes kontrol over oplysningerne.

Kommunen er dataansvarlig frem til det tidspunkt hvor anmoder har modtaget oplysninger. Herefter overgår dataansvar til anmoder.

Behandlingen af aktindsigten sker efter anmodning, hvorfor den må formodes at være forudsigelig for registrerede i de tilfælde hvor det er registrerede der er anmoder.

Data i løsningen indsamles via RPA, API eller manuelt upload fra sagsbehandleren. Kilderne er de fagsystemer, ESDH-systemer eller andre databærende systemer, som måtte indeholde data relevant for den pågældende aktindsigt.

## Modtagere af personoplysninger i AI-løsningen

I forbindelse med behandlingen af personoplysninger i AI-løsningen bliver personoplysninger videregivet til følgende modtagere:

I forbindelse med træning af modellen vil modtager af oplysninger være Aktio/leverandør. Platformen hostes på kommunens egne servere hvortil leverandøren har adgang via en VPN-forbindelse.
Nå AI løsningen implementeres vil modtager af oplysninger være sagsbehandler og aktindsigtsanmoder.

## Opbevaringsperiode for personoplysninger i AI-løsningen

Opbevaringsperioden for de personoplysninger, der behandles i AI-løsningen, er følgende:

I den periode, hvor aktindsigtsanmodningen behandles, vil dokumenter opbevares i den dertil beregnede IT-platform. Platformen hostes på kommunernes egne servere. Ved endt behandling journaliseres aktindsigten i ESDH-system, og slettes fra IT-platformen, uigenkaldeligt.

I forbindelse med udvikling, træning og test af AI-modellerne opbevares data i projektperioden så længe det vurderes at der er et formål med opbevaringen.

# Trin 2: Inddragelse af relevante interessenter

## Inddragelse af kommunens databeskyttelsesrådgiver (DPO)

Det følger af databeskyttelsesforordningen, at den dataansvarlige skal rådføre sig med sin databeskyttelsesrådgiver i forbindelse med udarbejdelsen af konsekvensanalyser.

Er kommunens databeskyttelsesrådgiver blevet hørt og inddraget i forbindelse med udarbejdelsen af denne konsekvensanalyse?

☒ Ja

☐ Nej

Databeskyttelsesrådgiveren har følgende bemærkninger:

AI-løsningen udvikles til at understøtte kommunens ansatte, der behandler aktindsigt anmodninger samt har brug for at udtrække dokumenter i forbindelse med en indsigtsanmodning efter databeskyttelsesforordningen.
En væsentlig opgave i forbindelse med implementeringen af løsningen vil være at fastholde medarbejdernes opmærksomhed på det fremsøgte resultat, således de forholder sig kritisk til den dokumentation, som løsningen foreslår samt være opmærksom på de gældende lovgivninger for aktindsigt. Især er det væsentligt at have opmærksomhed på, at Offentlighedsloven kan overrule GDPR lovgivning samt at være ekstra opmærksom på borgere med navne- og adressebeskyttelse.

# Indhentning af de registreredes eller deres repræsentanters synspunkter

Det følger af databeskyttelsesforordningens artikel 35, stk. 9, at det i nogle tilfælde er relevant at indhente de registreredes eller deres repræsentanters synspunkter. Dette afhænger af en konkret vurdering, som skal foretages og dokumenteres under dette afsnit.

Er de registreredes eller deres repræsentanters synspunkter indhentet og inddraget i forbindelse med udarbejdelsen af denne konsekvensanalyse?

☐ Ja

☒ Nej

Kommunerne er, som offentlig institution, forpligtet til at udføre en behandling af personoplysninger i forbindelse med aktindsigtsanmodninger. AI-løsningen er med til at løfte denne opgave i form af beslutningsstøtte, og der træffes ikke endelige afgørelser uden menneskelig indblanding. AI-løsningen bidrager til at sikre flere korrekte afgørelser, hvor der gives de oplysninger, der skal, hvormed antallet af sikkerhedsbrud også begrænses.  Dette er også i de registreredes egen interesse.

I henhold til databeskyttelsesforordningens artikel 86 må kommunen videregive personoplysninger i officielle dokumenter i forbindelse med aktindsigt.

Personoplysninger anvendes til træning af modellen i forbindelse med en aktindsigtsanmodning, hvorfor det vurderes at personoplysninger behandles i henhold til databeskyttelsesforordningens artikel 6, stk. 1, litra e, artikel 9, stk. 2, litra a, b, c, f, g, h og j samt databeskyttelsesloven § 8, stk. 1 og eventuelt § 11, stk. 1 for så vidt angår almindelige oplysninger, følsomme oplysninger, oplysninger om strafbare forhold og CPR-nummer. CPR-nummer bør dog så vidt muligt slettes fra afgørelserne inden, at de anvendes til test

og træning. Det vurderes, at behandling af fortrolige oplysninger kan behandles med hjemmel i straffelovens § 152 sammenholdt med Forvaltningslovens § 27.

Projektet er offentliggjort på Digitaliseringsstyrelsens hjemmeside, og informationer om projektaktiviteter offentliggøres løbende på projektets dertil beregnede hjemmeside. Derudover suppleres med blandt andet pressemeddelelser, artikler og oplæg på fagmesser. Disse kommunikative tiltag skal understøtte offentlig viden om projektet.

Det vurderes med udgangspunkt i ovenstående, at de registreredes eller deres repræsentanters synspunkter ikke skal inddrages.

# Trin 3: Projektets lovlighed, nødvendighed og proportionalitet

## Princippet om lovlighed, rimelighed og gennemsigtighed

Personoplysninger skal behandles lovligt, rimeligt og på en gennemsigtig måde i forhold til den registrerede, jf. databeskyttelsesforordningens artikel 5, stk. 1, litra a.

*Kravet om lovlighed*
Sønderborg Kommune efterlever princippet om lovlighed, idet personoplysninger i AI-løsningen behandles i henhold til databeskyttelsesforordningen artikel 6, stk. 1, litra e for så vidt angår almindelige personoplysninger, artikel 9, stk. 2, litra a, b, c, f, g, h og j for så vidt angår særlige kategorier af personoplysninger samt databeskyttelsesloven § 8, stk. 1 for så vidt angår strafbare forhold og eventuelt § 11, stk. 1 for så vidt angår CPR-nummer.
Det vurderes, at behandling af fortrolige oplysninger kan behandles med hjemmel i straffelovens § 152 sammenholdt med Forvaltningslovens § 27.
Dertil kommer databeskyttelsesforordningen artikel 86 om videregivelse af oplysninger ved aktindsigt.

*Kravet om rimelighed*
Sønderborg Kommune lever op til princippet om rimelighed, idet enhver aktindsigtsbehandling kræver stillingtagen i forhold til hvilke oplysninger, der kan udleveres samt de retslige grundlag for udlevering. AI-løsningen udvikles som støtte til behandling af de oplysninger, som udleveres. Med beslutningsstøtten vil sagsgangen effektiviseres, så behandlingstiden nedsættes og kontrollen af, at der alene udleveres korrekte oplysninger, øges. Dermed søges risiko for sikkerhedsbrud mindsket.
Modellens opgave er alene at fremsøge informationer og dokumenter til sagsbehandlers afgørelse af relevant materiale samt understøtte de registreredes rettigheder. Det er sagsbehandler, der udfører myndighedsopgaven.

*Kravet om gennemsigtighed*
Sønderborg Kommune skal med udgangspunkt i lovgivning for aktindsigter afgøre hvilken dokumentation, der kan udleveres. Der udarbejdes dokumentation for at imødekomme eller afvise en aktindsigtsanmodning
Personoplysninger trækkes fra de journaliserings- og/eller fagsystemer, hvori de behandles, hvilket den registrerede er gjort bekendt med ved oplysningspligten.

# Princippet om formålsbegrænsning

Personoplysninger skal indsamles til udtrykkeligt angivne og legitime formål og må ikke viderebehandles på en måde, der er uforenelig med disse formål. I denne forbindelse anses viderebehandling til arkivformål i samfundets interesse, til videnskabelige eller historiske forskningsformål eller til statistiske formål efter forordningens artikel 89, stk. 1, ikke at være uforenelige med de oprindelige formål, jf. databeskyttelsesforordningens artikel 5, stk. 1, litra b.

Personoplysninger behandles til træning af AI løsningen med udgangspunkt i genkendelighedslæring og ikke samkøring eller samstilling af indhold. De enkelte personoplysninger optræder således uden for oprindelig sammenhæng. Der anvendes både offentlige og interne data til træning.

Formålet med anvendelse af AI løsningen er alene at understøtte behandlingen af aktindsigtssager. AI løsningen understøtter dermed en behandlingsaktivitet, som er inden for kommunens forvaltningsområder, og som sker på baggrund af gældende lovgivning jf. offentlighedsloven, forvaltningsloven mv.

I forhold til brug af data til træning af løsningen svarer datatilsynet efter forespørgsel at:
*"I lige præcis forholdet til aktindsigt er det Datatilsynets opfattelse, at alene scopet for indsigten efter offentlighedsloven, sætter begrænsningen for hvilke dokumenter der kan udsøges. Der kan derfor lovligt ske behandling af alle oplysninger, der er i scope for anmodningen, med henblik på at vurdere om der skal ekstraheres heri eller ej."*

# Princippet om dataminimering

Personoplysninger skal være tilstrækkelige, relevante og begrænset til, hvad der er nødvendigt i forhold til de formål, hvortil de behandles, jf. databeskyttelsesforordningens artikel 5, stk. 1, litra c.

Sønderborg Kommune vil i forbindelse med en aktindsigtsanmodning forholde sig til de relevante dokumenter og personoplysninger, som kan udleveres til anmoder i henhold til lovgivning for aktindsigt.

AI-modellen trænes til at understøtte sagsbehandler i at fremfinde eventuelle oplysninger – herunder personoplysninger, som skal overstreges inden aktindsigtsanmodningen kan fremsendes. I forbindelse

med træning vil der være et stort behov for data fra tidligere aktindsigter, som skal bidrage til modellens træfsikkerhed.

## Princippet om rigtighed

Personoplysninger skal være korrekte og om nødvendigt ajourførte; der skal tages ethvert rimeligt skridt for at sikre, at personoplysninger, der er urigtige i forhold til de formål, hvortil de behandles, straks slettes eller berigtiges, jf. databeskyttelsesforordningens artikel 5, stk. 1, litra d.

Sønderborg Kommune kan jf. Databeskyttelseslovens § 11 benytte CPR-nummer, som unik identifikator, hvilket benyttes i løsningen.
AI-løsningen fremfinder dokumenter, som sagsbehandler kan gennemgå på baggrund af anmodningen, men sagsbehandler skal stadig vurdere om fremsøgningen har eventuelle mangler.
AI-løsningen er designet på en sådan måde, at den understøtter sagsbehandler ved gennemgang af sagsdokumenter, for at sikre kun de korrekte og lovlige oplysninger indgår i den dokumentation, der fremsendes ved en aktindsigtsanmodning. Det er sagsbehandlers ansvar at tjekke at alle informationer der skal udelades, er identificeret.
AI-løsningen designes for at fremme princippet om rigtighed ved aktindsigtsanmodninger.

## Princippet om opbevaringsbegrænsning

Personoplysninger skal opbevares på en sådan måde, at det ikke er muligt at identificere de registrerede i et længere tidsrum end det, der er nødvendigt til de formål, hvortil de pågældende personoplysninger behandles, jf. databeskyttelsesforordningens artikel 5, stk. 1, litra e.

Behandlede aktindsigter journaliseres, og slettes efter gældende lovgivning. Behandlede aktindsigter slettes uigenkaldeligt fra platformen. I trænings-/udviklingsfasen foretages der ikke sletning idet data skal bruges i træningen. Ved overgang til drift implementeres sletteprocedure.

Det sikres at denne praksis efterleves som en del af ledelseserklæringen som beskrevet i databehandleraftalen.

## Princippet om integritet og fortrolighed (sikkerhed og robusthed)

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, under anvendelse af passende tekniske eller organisatoriske foranstaltninger, jf. databeskyttelsesforordningens artikel 5, stk. 1, litra f.

Det følger endvidere af databeskyttelsesforordningens artikel 32, at den dataansvarlige skal gennemføre passende tekniske og organisatoriske foranstaltninger for at sikre det fornødne sikkerhedsniveau i AI-løsningen.

Sønderborg Kommune har udarbejdet en risikovurdering for AI-løsningen og endvidere indgået de nødvendige databehandleraftaler, hvori indgår fastlæggelse af tilstrækkelige tekniske og organisatoriske foranstaltninger med udgangspunkt i de personoplysninger, som løsningen behandler.

Kommunernes udpegede IT-medarbejdere har adgang til dette software. I projektperioden vil leverandøren ligeledes have adgang. Brugerstyring sker gennem en Single Sign-on adgang til platformen.

# Behandlingsgrundlag (hjemmel)

Behandling af personoplysninger skal have et behandlingsgrundlag (hjemmel) i databeskyttelsesforordningen, databeskyttelsesloven eller særlovgivningen.

Sønderborg Kommune udvikler AI-løsningen, som støtte til aktindsigtsbehandling og dermed vurderes det, at der er behandlingshjemmel, som beskrevet i afsnittet omkring lovlighed af behandlingen.

# De registreredes rettigheder

## Registreredes ret til underretning (oplysningspligten)

Det følger af databeskyttelsesforordningens artikel 13 og 14, at registrerede som udgangspunkt har ret til en række oplysninger om behandlingen af deres personoplysninger. Disse oplysninger skal meddeles den registrerede, uanset om oplysningerne er indsamlet fra den registrerede selv eller fra andre end den registrerede selv.

I henhold til databeskyttelsesforordningens artikel 86 må Kommunen videregive personoplysninger ved aktindsigtssager, hvorfor det vurderes, at de registrerede ikke skal informeres om behandlingen af deres personoplysninger ved udviklingen af en model til støtte for en sådan behandling.

Det vil kræve en uforholdsmæssig stor indsats at oplyse de registrerede om dette udviklings- og træningsformål henset til antallet af registrerede at oplysningerne også er pseudonymiseret og at de registreredes interesse i at få denne orientering ikke kan antages at være stor (artikel 14, stk. 5, litra b).

## Indsigtsretten

Det følger af artikel 15, at registrerede som udgangspunkt har ret til at se de personoplysninger, som den dataansvarlige behandler om dem – og ligeledes har registrerede ret til at få en kopi med oplysningerne

udleveret gratis. Derudover har registrerede ret til at få en række oplysninger om, hvordan deres personoplysninger behandles, samt hvor de stammer fra. På den måde sikres behandlingsaktivitetens gennemsigtighed.

Sønderborg Kommune understøtter indsigtsretten efter databeskyttelsesforordningens artikel 15 for så vidt angår den nuværende sagsbehandling og afgørelse, samt for de data, der indgår i modellens understøttende database.

Træningsdata består af data fra fagsystemer, ESDH systemer og andre løsninger, hvorfra der kan anmodes om aktindsigt. Der er ikke indhentet yderligere data. Data er ikke blevet anonymiseret i træningsperioden. I selve løsningen minimeres personoplysninger i videst muligt omfang til kun at omfatte formålet med behandlingen.

## Berigtigelsesretten

Det følger af artikel 16, at registrerede som udgangspunkt har ret til at få forkerte oplysninger om dem selv rettet. De har derudover ret til at få gjort deres ufuldstændige personoplysninger fuldstændige. I tilfælde af rettelser skal den dataansvarlige være i stand til at underrette eventuelle modtagere af personoplysningerne om oplysningernes ændring.

Sønderborg Kommune anvender alene data, hvor parterne har haft mulighed for at berigtige data.
Sønderborg Kommune ændrer ikke i disse data.
Eventuelle ændringer i fagsystemet, der sker uafhængigt af AI-løsningen, vil blive opdateret i sagsdatabasen.

## Registreredes ret til sletning (retten til at blive glemt), ret til begrænsning, ret til dataportabilitet og indsigelsesret

De registrerede har en række øvrige rettigheder, herunder ret til sletning (artikel 17), ret til begrænsning af behandlingen (artikel 18), ret til dataportabilitet (artikel 20) og indsigelsesret (artikel 21).

Sønderborg Kommune har pligt til at opbevare personoplysninger i minimum 5 år fra sagsafslutning i forbindelse med overholdes af databeskyttelseslovens artikel 6, stk. 1, litra e og er således undtaget ret til sletning jf. databeskyttelsesforordningen artikel 17, stk. 3, litra b.

Ret til begrænsning af behandling jf databeskyttelsesforordningens artikel 18, skal efterleves for så vidt en registreret ikke ønsker, at vedkommendes sagsakter indgår i sagsdatabasen. Ved en henvendelse fra den registrerede skal sagen straks fjernes fra sagsdatabasen. Sagen vil dog stadig skulle opbevares i henhold til opbevaringforpligtelsen

Ret til dataportabilitet jf. databeskyttelsesforordningens artikel 20, stk. 3 vurderes ikke at være relevant.

Ret til indsigelse jf. databeskyttelsesforordningens artikel 21, stk. 1, skal efterleves for så vidt en registreret ikke ønsker, at vedkommendes sagsakter indgår i sagsdatabasen. Ved en henvendelse fra den registrerede skal sagen straks fjernes fra sagsdatabasen. Sagen vil dog stadig skulle opbevares i henhold til opbevaringsforpligtelsen. Retten til indsigelse er ikke gældende for den behandling, der er nødvendig for at træffe en afgørelse i henhold til særlovgivningen, samt i forhold til statistik/forskning.

### Registreredes ret til ikke at være genstand for automatiske individuelle afgørelser

Det følger af artikel 22, at den dataansvarlige som udgangspunkt ikke må gøre registrerede til genstand for afgørelser, der alene er baseret på automatisk behandling (herunder profilering), som har retsvirkning eller på tilsvarende vis betydeligt påvirker registrerede, dvs. fuldautomatiske afgørelser uberørt af menneskehånd. Denne rettighed finder dog bl.a. ikke anvendelse, hvis afgørelsen har hjemmel i dansk lov eller EU-retten, jf. artikel 22, stk. 2, litra b. I så fald kan de automatiske individuelle afgørelser lovligt finde sted.

Forholdet omkring *automatiske individuelle afgørelser* vurderes Ikke at være relevant. Løsningen giver ikke forslag til afgørelse af sagerne. Løsningen fungerer udelukkende til støtte til et menneske som træffer afgørelsen.

## Databehandlere

Anvender kommunen en eller flere databehandlere til behandlingen af personoplysninger i AI-løsningen?

☒ Ja

☐ Nej

I forbindelse med projektet har Sønderborg Kommune indgået aftale med Aktio om udvikling af NLP-modeller til beslutningsstøtte i forbindelse med behandling af aktindsigter. Databehandler har adgang til data i forbindelse med udvikling af AI-løsningen. Der er i databehandleraftalen pålagt et tilstrækkeligt sikkerhedsniveau.
Der er indgået databehandleraftale med ovenstående formål og udarbejdet en risikovurdering med udgangspunkt i konsekvenser for både organisationen og de registrerede i forhold til Fortrolighed, Integritet og Tilgængelighed.

Databehandler leverer årligt en ledelseserklæring med reference til ISAE 3000 og dataansvarlig har mulighed for at foretage tilsyn.

Aktio bruger underdatabehandler Alvenir til udviklingen af sprogmodellerne. Krav til tilsyn med underdatabehandler fremgår af databehandleraftale og indgår som led i årlig ledelseserklæring. Aktio anvender ligeledes underdatabehandleren Kvalitets-IT til Single Sign-on til platformen Aktio Indsigt.

## Overførsel til tredjelande og/eller internationale organisationer

Overfører kommunen personoplysninger til tredjelande og/eller internationale organisationer i forbindelse med behandling af personoplysninger i AI-løsningen, f.eks. ved brug af cloud computing, dataanalyse, support m.v.?

☐ Ja

☒ Nej

# Trin 4: Identifikation, evaluering og håndtering af risici

Næste skridt er at *identificere* behandlingsaktivitetens risici for de registreredes rettigheder og frihedsrettigheder (risikoidentifikation), *evaluere* og beskrive disse risici ud fra deres sandsynlighed og alvor (risikoevaluering) samt *håndtere* risiciene ved hjælp af afhjælpende foranstaltninger, jf. databeskyttelsesforordningens artikel 35, stk. 7, litra c-d. Formålet med de afhjælpende foranstaltninger er at nedbringe de identificerede risici til et acceptabelt niveau. De typiske risikostyringsstrategier vil være at enten eliminere, reducere eller acceptere den identificerede risiko.

Det er vigtigt at være opmærksom på, at en risiko ikke nødvendigvis behøver at være en *sikkerhedsmæssig* risiko, dvs. en risiko vedrørende (utilstrækkelig) behandlingssikkerhed, f.eks. ulovlig adgang internt og eksternt til personoplysninger m.v. En risiko kan tillige vedrøre manglende overholdelse af øvrige af forordningens regler, f.eks. risikoen for dataophobning, overdreven indsamling af personoplysninger, der ikke er proportional med formålet, uønskede ændringer og forsvundne personoplysninger, ulovlig viderebehandling af personoplysninger eller manglende overholdelse af de registreredes rettigheder m.v.

Eksempler på konsekvenser for den registrerede kan f.eks. være fysisk, materiel eller immateriel skade, forskelsbehandling, identitetstyveri eller -svig, finansielle tab, skade på omdømme, tab af fortrolighed for personoplysninger, der er omfattet af tavshedspligt, uautoriseret ophævelse af pseudonymisering eller andre betydelige økonomiske eller sociale konsekvenser, samt hvis de registrerede kan blive berøvet deres rettigheder og frihedsrettigheder eller forhindret i at udøve kontrol med deres personoplysninger, jf. databeskyttelsesforordningens præambelbetragtning 75.

## Valg af evalueringskriterier for sandsynlighed og konsekvens

En risiko defineres i denne konsekvensanalyse som et scenarie, der beskriver en hændelse og konsekvenserne heraf, som vurderes i forhold til alvor og sandsynlighed. I forbindelse med risikoevalueringen skal der derfor foretages en vurdering af risikoens sandsynlighed og konsekvens. Vurderingen skal foretages for hver enkelt identificeret risiko set ud fra den registreredes perspektiv, men på et objektivt grundlag.

I denne konsekvensanalyse anvendes følgende evalueringskriterier for sandsynlighed:

*Tabel 1. Evalueringskriterier for sandsynlighed*

| | |
|---|---|
| **4** | **Forventet**: Det forventes, at hændelsen vil forekomme, herunder f.eks.:<br>- Man har erfaring med hændelsen inden for de sidste 12 måneder<br>- Hænder jævnligt hos andre offentlige myndigheder og private virksomheder (omtales ofte i pressen) |
| **3** | **Sandsynligt**: Det er moderat sandsynligt, at hændelsen vil forekomme, herunder f.eks.:<br>- Man har erfaring med hændelsen, men ikke inden for de sidste 12 måneder<br>- Kendes fra andre offentlige myndigheder og private virksomheder i Danmark (omtales i pressen) |
| **2** | **Mindre sandsynligt**: Hændelsen forventes ikke at forekomme, herunder f.eks.:<br>- Ingen erfaring med hændelsen<br>- Kendes fra få andre offentlige myndigheder og private virksomheder, men ikke i Danmark |
| **1** | **Usandsynligt**: Det anses for næsten udelukket, at hændelsen nogen sinde kan forekomme, herunder f.eks.:<br>- Ingen erfaring med hændelsen<br>- Kendes fra få andre offentlige myndigheder og private virksomheder, men ikke i Danmark |

I denne konsekvensanalyse anvendes følgende evalueringskriterier for konsekvens[2]:

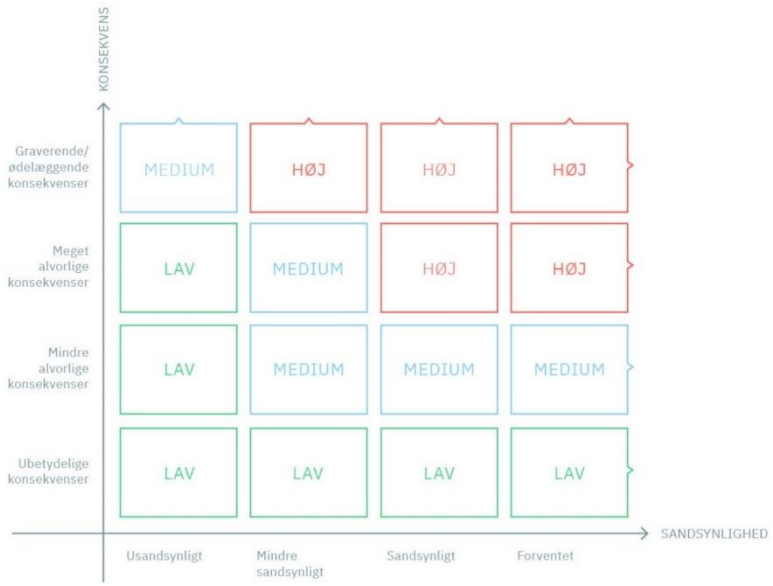
*Tabel 2. Evalueringskriterier for konsekvens*

| | |
|---|---|
| **4** | **Graverende/ødelæggende konsekvenser**: De registrerede kan opleve kritiske konsekvenser, som de ikke nødvendigvis kan overvinde, f.eks. økonomisk nød som betydelig gæld eller manglende evne til at arbejde, langsigtede psykiske eller fysiske lidelser, død m.v. |
| **3** | **Meget alvorlige konsekvenser**: De registrerede oplever betydelige konsekvenser, som de kan overvinde om end med alvorlige vanskeligheder, f.eks. identitetstyveri eller -svig, finansielle tab, blacklisting af banker, ejendomsskade, tab af beskæftigelse, stævning, forværring af sundhedstilstanden, tab af fortrolighed af personoplysninger, der er omfattet af tavshedspligt m.v. |
| **2** | **Mindre alvorlige konsekvenser**: De registrerede oplever begrænsede konsekvenser, som de vil være i stand til at overvinde med få vanskeligheder, f.eks. ekstra omkostninger, nægtelse af adgang til forretningstjenester, manglende forståelse, frygt, stress, mindre fysiske påvirkninger m.v. |
| **1** | **Ubetydelige konsekvenser** De registrerede bliver enten ikke påvirket eller udsættes alene for få generende konsekvenser, som de uden problemer kan håndtere, f.eks. tidsforbrug brugt på at genindtaste oplysninger, irritationer, dårlig brugeroplevelse m.v. |

[2] Se f.eks. punkt A.2 i Annex A til ISO/IEC 29134:2017, Information technology - Security techniques - Guidelines for privacy impact assessment; Datatilsynet m.fl., Vejledning om behandlingssikkerhed og databeskyttelse gennem design og standardindstillinger, juni 2018, s. 9; samt Digitaliseringsstyrelsen, Vejledning i vurdering af offentlige it-projekters potentielle konsekvenser for privatlivet, maj 2013, s. 12

Når evalueringskriterierne for sandsynlighed og konsekvens er fastlagt, kan hver enkelt identificeret risiko vurderes og kortlægges på et såkaldt risikokort. I denne konsekvensanalyse anvendes følgende risikokort:

*Figur 1. Risikokort*




# Identifikation, evaluering og håndtering af behandlingsaktivitetens konkrete risici

Den samlede risikovurdering er vedlagt denne DPIA som bilag. I denne er samtlige risici beskrevet i Risikokataloget gennemgået og vurderet. I forhold til behandlingssikkerheden henvises til artikel 32 som vurderes opfyldt ved denne DPIA, den interne risikovurdering af projektet samt opfølgning på disse.

Af tabel 1 fremgår en oversigt over de risici, der er vurderet til at have en risikoscore over 8. Risikoscoren er udregnet ved at gange sandsynlighed (1-4) med konsekvens (1-4). For hver risiko er der udpeget forebyggende og forbedrende foranstaltninger, som skal mindske risikoen. På baggrund af disse er sandsynlighed og konsekvens genvurderet, hvorefter en ny risikoscore (restrisikoscore) er beregnet.

*Tabel 1: Væsentligste risici*

| Risiko nr. | Risiko | Risikoscore | Forebyggende tiltag | Restrisiko |
|---|---|---|---|---|
| 2.2 | Risiko for, at brugerne ikke kender til AI systemets karakter, kompetencer og begrænsninger | 12 | • Uddannelse i brug af systemet<br>• Stopklodser undervejs i processen<br>• Vejledninger i brug af systemet | 6 |

| | | | | |
|---|---|---|---|---|
| 9.1 | Risiko for manglende eller utilstrækkelig afklaring af ansvar for og ledelsesmæssig godkendelse af udvikling og brug af AI-systemet | 12 | • Anvende dokumenterede retningslinjer<br>• Definerede ledelses- og ansvarsroller | 2 |
| 9.2 | Risiko for manglende eller utilstrækkelig uddannelse af centrale medarbejdere | 12 | • Procedure for opstart af nye medarbejdere<br>• Stopklodser indbygget i løsningen<br>• Vejledninger indbygget i løsningen | 4 |
| 9.4 | Risiko for uhensigtsmæssig lav kvalitet eller utilsigtede hændelser pga. utilstrækkelig testning, revision og overvågning af AI-systemet | 8 | • Etablering og vedligeholdelse af retningslinjer/vejledninger<br>• Gennemførsel af Audits og tilsyn (indgår i Ledelsestilsyn) | 4 |
| 6.1 | Risiko for manglende muligheder for effektiv rettighedsudøvelse for de registrerede | 8 | • Implementering af retningslinjer | 8 |

Herunder beskrives disse identificerede risici, samt de udpegede foranstaltninger.

### *2.2 Risiko for, at brugerne ikke kender til AI systemets karakter, kompetencer og begrænsninger*

Det udgør en risiko for brugerne af systemet, hvis de ikke har den information, det kræves for at forstå og interagere med AI-systemet i en tilfredsstillende grad, herunder vurdere systemets begrænsninger. Brugerne forstås her som de medarbejdere der anvender AI-løsningen som beslutningsstøtte i behandlingen af aktindsigt. Her kan manglende kendskab til brugen af løsningen udgøre en risiko for forkert brug af løsningen, for eksempel i form af manglende stillingtagen til forslag, misforståelse af systemets karakter samt manglende kendskab til systemets begrænsning kan blandt andet føre til at AI-løsningen reelt anvendes som et automatisk afgørelsesværktøj snarere end til beslutningsstøtte.

<u>Forebyggende organisatoriske tiltag</u>

Der udarbejdes vejledninger til medarbejderne som forklarer hvordan løsningen skal bruges, dens karakter samt de begrænsninger løsningen kan forventes at have. Derudover skal oplæring anvendes ved nye medarbejdere.

For at sikre forankring af disse vejledninger i driften udarbejdes og godkendes en rolle- og ansvarsbeskrivelse på ledelsesniveau.

<u>Tekniske foranstaltninger</u>

Der indbygges såkaldte "stopklodser" undervejs i processen i behandlingen af aktindsigten, som har til formål at minde sagsbehandler om, at de skal forholde sig til det, AI løsningen har fremsøgt. Inden behandlingen kan afsluttes, skal medarbejder bekræfte, at informationen er gennemset og korrekt.

Restrisikovurdering
Med implementering af ovenstående foranstaltninger vurderes det, at sandsynligheden for, at brugerne af systemet har manglende kendskab til systemets karakter og begrænsninger kan minimeres betragteligt. Således falder sandsynlighedsvurderingen fra 4 til 2, hvormed der er en restrisikoscore på 6

### *9.1 Risiko for manglende eller utilstrækkelig afklaring af ansvar for og ledelsesmæssig godkendelse af udvikling og brug af AI-systemet*

Hvis der ikke er en klar og kommunikeret fordeling af ansvar for og ledelsesmæssig godkendelse af udvikling og brug af AI-systemet, kan det medføre, at relevante beslutninger om AI-systemets udvikling, drift eller berostillelse er forkerte eller slet ikke tages. Tilsvarende gælder beslutninger vedrørende implementering og opfølgning på aftalte foranstaltninger.

Organisatoriske foranstaltninger
Der er implementeret en projektorganisation med styregruppe samt flere følgegrupper, som har ansvar for at sikre, at der sker godkendelse af udviklingstiltag, samt monitorering af disse, løbende i projektets levetid. Der er udarbejdet en projekttidsplan hvor milepæle og godkendelser fremgår.

Ved projektafslutning skal der foreligge en plan for, hvordan det sikres, at ansvar og roller forankres i en overgang til drift. Af denne ansvars- og rollefordeling skal det beskrives hvordan det sikres, at beskrevne procedurer for anvendelse følges.

Der laves en beskrivelse af systemets karakter, kompetencer og begrænsninger, hvori systemets anvendelsesmuligheder tydeligt fremgår.

Restrisiko
Det vurderes at ovenstående foranstaltninger kan medføre en reduktion i sandsynlighed, således at sandsynlighedsvurderingen falder fra 4 til 1. Dermed er der en restrisiko på 2.

### *9.2 Risiko for manglende eller utilstrækkelig uddannelse af centrale medarbejdere*

Hvis medarbejderne ikke er tilstrækkeligt uddannede i at håndtere AI-systemer og dets særegne databeskyttelsesretlige risici, er der risiko for medarbejderfejl og dermed overtrædelse af reglerne.

Organisatoriske foranstaltninger

Relevante medarbejdere, herunder AI-udviklere, projektleder og øvrige nøglepersoner, uddannes i systembrug. Der udarbejdes dokumenterbart materiale i forbindelse hermed, som anvendes ved træning af nye brugere.
Der udarbejdes retningslinjer for oplæring af nye medarbejdere, samt en roller- og ansvarsfordelingsbeskrivelse som skal sikre ledelsesmæssig forankring i de enkelte områder. (se risiko 2.2)
Der udarbejdes vejledende materiale til systembrugerne, hvori opmærksomhedspunkt i forhold til databeskyttelse beskrives.

Tekniske foranstaltninger
Der bygges vejledninger ind i platformen, som skal være med til at sikre medarbejdernes kendskab til de sprogmodeller, løsningen anvender til fremsøgning af oplysninger, og hvordan disse anvendes i praksis.

Der er fokus på involvering af de rette kompetencer gennem hele projektets livscyklus.

Restrisiko
De udpegede foranstaltninger vurderes at kunne mindske sandsynligheden for manglende eller utilstrækkelig uddannelse af centrale medarbejdere, således at vurderingen af sandsynlighed går fra 4 til 2.

### *9.4 Risiko for uhensigtsmæssig lav kvalitet eller utilsigtede hændelser pga. utilstrækkelig testning, revision og overvågning af AI-systemet*

Hvis der ikke foretages tilstrækkelig og dokumenterbare tests, revision og overvågning af AI-systemet både under udvikling og løbende i drift, er der risiko for manglende opdagelse af fejl og utilstrækkelig opfyldelse af kravene til systemet.

Organisatoriske foranstaltninger
Der er indgået en da Databehandleraftale, hvori krav til kvalitet testning, revision og overvågning af AI systemet er indskrevet.
Der stilles som krav i databehandleraftalen, at leverandøren laver årlige ledelseserklæringer, og det fremgår ligeledes, at dataansvarlig har mulighed for at gennemføre tilsyn.

Der etableres og vedligeholdes dokumenterbare retningslinjer og processer for test af AI-systemet før go live og med et passende interval efter go live samt ved ændringer. Gennemførte tests, resultater heraf samt foranstaltninger truffet i medfør heraf skal kunne dokumenters.

Restrisiko
Ved implementering af beskrevne foranstaltninger vurderes det, at sandsynligheden for at der er en uhensigtsmæssig lav kvalitet eller utilsigtede hændelser mindskes. Således falder sandsynlighedsvurderingen fra 3 til 2.

Den samlede restrisikoscore er på 4.

### *6.1 Risiko for manglende muligheder for effektiv rettighedsudøvelse for de registrerede*

Personoplysninger kan indgå i (1) træningsdata ved udvikling af systemet, (2) testdata ved test af systemet, (3) data i selve modellen, (4) inputdata ved anvendelse af systemet samt (5) outputdata ved anvendelse af systemet, f.eks. en afgørelse eller forudsigelse. De registreredes rettigheder skal kunne håndteres i forhold til alle disse anvendelser af personoplysninger. Dog kan det i praksis vise sig vanskeligt at imødekomme visse rettigheder i forbindelse med test- og træningsdata på grund af pseudonymisering.

Organisatoriske foranstaltninger

Der udarbejdes retningslinjer og procedurer for håndtering af de registreredes rettigheder både ved modeludvikling og ved overgang for drift. Dette medtages i de overordnede retningslinjer for anvendelse af systemet, uddannelsesmateriale/vejledninger samt i roller- og ansvarsfordelingsbeskrivelsen.

Tekniske foranstaltninger

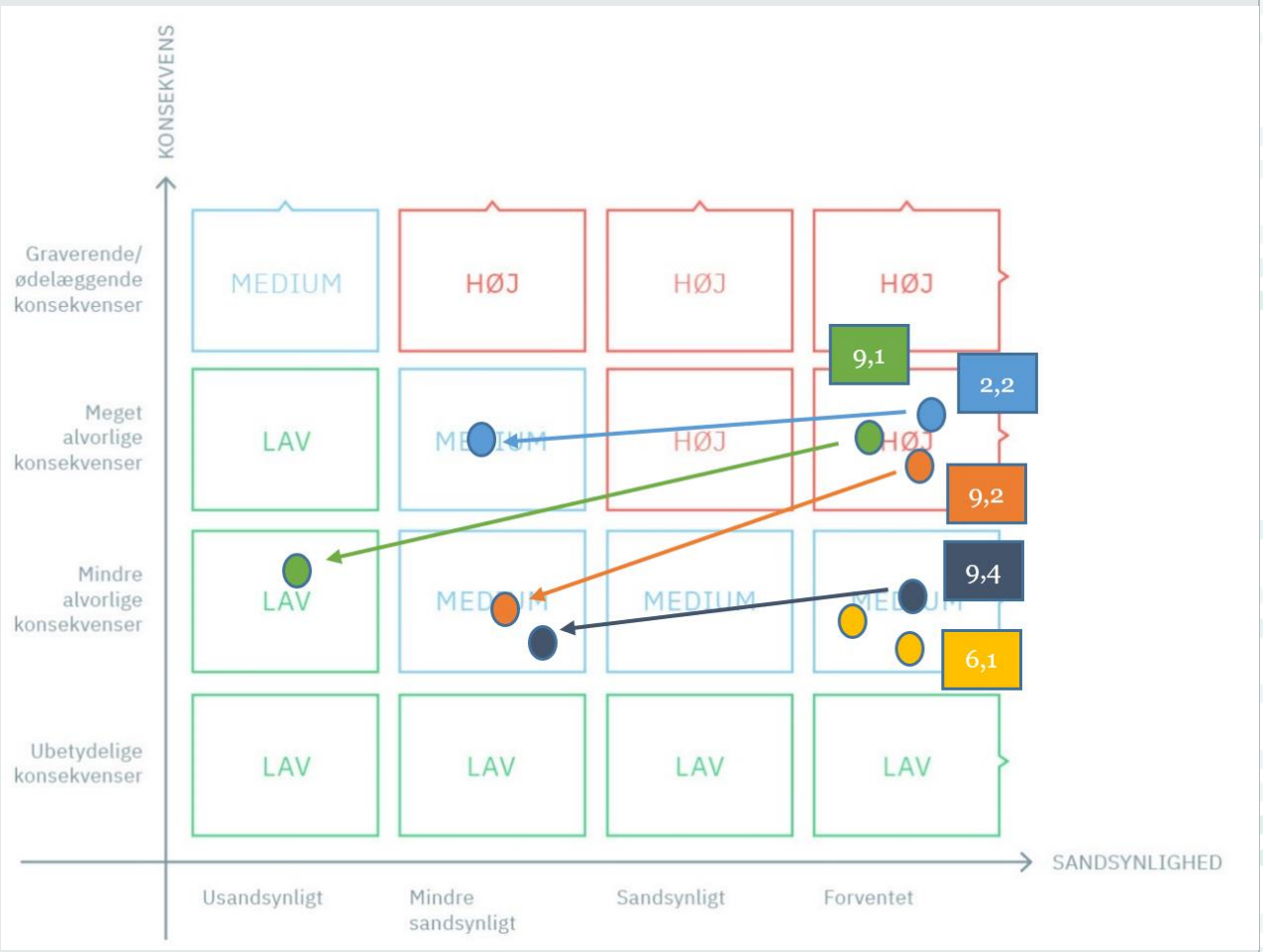
For at sikre, at data ikke kan føres tilbage til specifikke registrerede, hverken i forbindelse med træning af modellen, eller ved brug af testdata, anvendes Differential Privacy som metode til Pseudonymisering af data. Data samles ligeledes i batches.

Restrisiko

Sandsynlighed og konsekvens vurderes at være det samme med de implementerede foranstaltninger.

## *Risikokort*

Af figur fire fremgår de væsentligste risicis placeringer på risikokortet. Det fremgår ligeledes, hvordan risici placeres efter implementering af foranstaltninger (restrisiko).




*Figur 4: Risikokort - væsentligste risici*

## *Overordnet residualrisikovurdering*

Med implementering af de her beskrevne foranstaltninger, herunder dokumenterbare retningslinjer og processer i forhold til anvendelse af systemet, kendskab til muligheder og begrænsninger, roller-og ansvarsfordeling samt tilsyn og godkendelse i løsningens livscyklus, vurderes det, at løsningens overordnede restrisikoscore vil være inden for kategorien "lav-medium" i risiko-kortet.

Sønderborg Kommune: Der er lavet en intern risikovurdering med udgangspunkt i fortrolighed, integritet og tilgængelighed for forretningskonsekvens og de registreredes rettigheder. Håndtering foregår på direktionsniveau. Resultatet på vores interne risikovurdering vil være medium-høj.

# Trin 5: Konklusion og ledelsesgodkendelse

## AI-løsningens samlede restrisiko og høring af Datatilsynet

På baggrund af de samlede risikoscorer *efter* afhjælpende foranstaltninger (sidste række i tabellen ovenfor), som du har vurderet og angivet under håndteringen af de enkelte identificerede risici, skal du her vurdere den samlede rest-risiko for behandlingen af personoplysninger i AI-løsningen.

Den samlede restrisiko for behandlingsaktiviteten *efter afhjælpende foranstaltninger* vurderes at være:

☐ Høj

☒ Medium

☒ Lav

Med implementering af de her beskrevne foranstaltninger, herunder dokumenterbare retningslinjer og processer i forhold til anvendelse af systemet, kendskab til muligheder og begrænsninger, roller-og ansvarsfordeling samt tilsyn og godkendelse i løsningens livscyklus, vurderes det, at løsningens overordnede restrisikoscore vil være inden for kategorien "lav-medium" i risiko-kortet.

## Ledelsens godkendelse af konsekvensanalysen

| | | |
|---|---|---|
| ☒ | Godkendt | Behandlingsaktiviteten kan påbegyndes, hvis de afhjælpende foranstaltninger i **Handlingsplanen** (**Bilag 2**) bliver gennemført. |
| ☐ | Betinget godkendt | Behandlingsaktiviteten kan kun påbegyndes, hvis nærmere beskrevne ændringer foretages. Efter den betingede godkendelse |

| | | |
|---|---|---|
| | | skal ledelsen præsenteres for en ny, revideret konsekvensanalyse med henblik på endelig godkendelse. |
| ☐ | Ikke godkendt | Behandlingsaktiviteten kan ikke gennemføres. |

Begrundelsen for ledelsens valg i forhold til godkendelse er følgende:

Ledelsen godkender denne DPIA med begrundelsen:

- Risikoniveauet ligger inden for det acceptable i Sønderborg Kommune.
- Relevante parter, herunder datatilsynet samt kammeradvokaterne, har været inddraget i processen med udarbejdelse af denne DPIA.

Vurderer ledelsen, at konsekvensanalysen skal offentliggøres enten helt eller delvist?

☒ Ja, konsekvensanalysen skal offentliggøres i sin helhed

☐ Ja, konsekvensanalysen skal delvist offentliggøres

☐ Nej, konsekvensanalysen skal ikke offentliggøres

Begrundelsen for ledelsens valg i forhold til offentliggørelse er følgende:

Ledelsen vurderer at DPIA'en med fordel kan offentliggøres, da den er udarbejdet i forbindelse med et Signaturprojekt, som har til formål at styrke kendskab til brugen af Kunstig Intelligens.

Ved fremtidige ændringer tages der stilling til, hvorvidt den opdaterede DPIA ligeledes offentliggøres. DPIA'en forholder sig til projektet, og ikke til fremtidig ibrugtagning og efterfølgende drift.

DPIA'en afspejler et øjebliksbillede ved offentliggørelsen af denne.

DPIA'en offentliggøres på projektets hjemmeside.

# Bilag til konsekvensanalysen

Følgende bilag vedlægges eventuelt til konsekvensanalysen:

☒ Skema til identifikation, evaluering og håndtering af risici (**Bilag 1**)

☒ Risikovurdering vedrørende behandlingssikkerhed efter databeskyttelsesforordningens artikel 32

☐ Andre (indsættes i kommentarboks nedenfor):

*[Indsæt titler på øvrige bilag, der vedlægges konsekvensanalysen]*

# Trin 6: Ajourføring af konsekvensanalysen

Kommunen skal regelmæssigt gennemgå konsekvensanalysen vedrørende databeskyttelse og de behandlingsaktiviteter, som vurderes i denne, jf. databeskyttelsesforordningens artikel 35, stk. 11.

Denne konsekvensanalyse vedrørende databeskyttelse skal fremadrettet ajourføres efter følgende procedure:

| |
|---|
| Der følges op på DPIA'en helårligt samt ved væsentlige ændringer eller hændelser. |

# Bilag

**Bilag 1**: Risikovurdering