|  |
| --- |
| **Juridisk værktøjskasse for Ansvarlig AI**  **Værktøj nr. 4**  Katalog over krav til AI-løsningen |

Indhold

[1. Introduktion til kravkataloget 3](#_Toc43917174)

[1.1 Formålet med kravkataloget 3](#_Toc43917175)

[1.2 Indhold og anvendelsesområdet for kravkataloget 4](#_Toc43917176)

[1.3 Behov for supplering og tilpasning 5](#_Toc43917177)

[2. del I: krav til løsningen efter særlovgivningen 7](#_Toc43917178)

[3. del II: forvaltningsretlige krav til løsningen 8](#_Toc43917179)

[4. Del III: databeskyttelsesretlige krav til løsningen 9](#_Toc43917192)

[4.1 Databeskyttelsesretlige krav 9](#_Toc43917193)

[4.2 Designprincipper vedrørende databeskyttelse 16](#_Toc43917194)

[5. del IV: Væsentlige immaterialretlige krav (rettighedsbestemmelser) 19](#_Toc43917195)

[5.1 Rettighedsbestemmelser til den software, der indgår i AI-systemet 19](#_Toc43917196)

[5.2 Rettighedsbestemmelser til de data, der benyttes i AI-løsningen 22](#_Toc43917197)

[5.3 Rettighedsbestemmelser til de resultater, der kommer ud af at benytte AI-løsningen 23](#_Toc43917198)

# Introduktion til kravkataloget

## Formålet med kravkataloget

Det er et grundlæggende krav, at kommunernes AI-løsninger overholder gældende relevant lovgivning, dvs. kan understøtte en korrekt anvendelse af reglerne. Det er den enkelte kommunes ansvar, at de AI-løsninger, som de benytter, overholder de retlige krav i hele AI-løsningernes livscyklus. Dette gælder uanset, om der er tale om standardløsninger eller løsninger, der er udviklet specielt til en bestemt opgave hos en eller flere kommuner.

For at undgå fordyrende ændringer eller forsinkende tilbageløb i udviklingsprocessen, er det vigtigt, at de relevante regler identificeres og tænkes ind i løsningen så tidligt som muligt i udviklingen.

Formålet med dette kravkatalog er at understøtte kommunen i denne opgave, dvs. udvikling af hensigtsmæssige AI-løsninger, der overholder de retlige krav efter lovgivningen. Det gælder særligt de retlige krav og designprincipper efter reglerne om indbygget databeskyttelse og databeskyttelse som standardindstillinger i databeskyttelsesforordningen og -loven, samt at understøtte en effektiv håndtering af databeskyttelsesrisici for de registrerede.

Kravkataloget er således tænkt som et værktøj, hvor kommunen kan opliste de identificerede krav til løsningen og dermed løbende dokumentere over for relevante interessenter og tilsynsmyndigheder, at AI-løsningen er designet til at overholde den relevante lovgivning af betydning for løsningen.

Kravkataloget kan både anvendes af kommuner, der selv udvikler AI-løsningen (egenudvikling), samt af kommuner, der enten køber en standardløsning eller en skræddersyet løsning fra en leverandør.

* Hvis kommunen anvender en ekstern leverandør, kan kommunen tillige bruge kravkataloget som inspiration, når kommunen skal stille krav til leverandøren af AI-løsningen i en kravspecifikation i en it-kontrakt, typisk i forbindelse med en udbudsproces.
* Køber kommunen en standardløsning, kan kommunen bruge kravkataloget som en tjekliste til overvejelse af, om AI-løsningen lever op til de retlige krav.

Derudover tjener kravkataloget følgende yderligere formål:

* Kan understøtte forventningsafstemninger mellem kommunen og leverandører
* Kan bruges som dokumentation (eksempelvis ved tilsyn) for, at der stilles relevante databeskyttelsesretlige krav til leverandører, f.eks. krav om dataminimering og transparens
* Kan anvendes ved ekstern og intern auditering eller ved tilsyn og revision
* Kan tjene som generel inspiration til kommunens arbejde med databeskyttelse i forbindelse med brug af AI.

## Indhold og anvendelsesområdet for kravkataloget

Kravkataloget indeholder retlige krav fordelt på 4 dele som følger:

1. Krav til løsningen efter særlovgivningen
2. Forvaltningsretlige krav til løsningen
3. Databeskyttelsesretlige krav til løsningen
4. Immaterialretlige krav (rettighedsbestemmelser til it-kontrakten)

Del IV vedrører immaterialretlige krav, der kan være relevante at adressere inden udviklingen af AI-løsningen, herunder bl.a. i forhold til hvem der skal have rettighederne til AI-løsningen, dens data og dens resultater. Kravene kan bruges til at indarbejde i it-kontrakten med udviklingsleverandøren.

Kravkataloget indeholder *systemmæssige krav*, dvs. krav til selve AI-løsningens funktionalitet. I kravkataloget skal således ikke dokumenteres krav i form af organisatoriske foranstaltninger under udviklingen og anvendelsen af løsningen, f.eks. krav om den fornødne governance og hjemmel for behandlingen samt interne retningslinjer for håndtering af de registreredes rettigheder m.v. Håndteringen af sådanne organisatoriske foranstaltninger er – for så vidt angår databeskyttelsesretlige krav – håndteret i værktøjskassens øvrige værktøjer.

Kravkataloget indeholder krav vedrørende *udvikling* af AI-løsninger, og ikke den efterfølgende *drift* af AI-løsningen, hvor det typisk vil være relevant at forholde sig til sikkerhedskrav til driften af løsningen, herunder behandling af personoplysninger i forbindelse med support og hosting i en databehandleraftale m.v.

## Behov for supplering og tilpasning

Kommunerne skal selv udfylde kravkataloget for så vidt angår krav til løsningen efter særlovgivningen og forvaltningsretten efter anvisningerne i kravkatalogets Del I-II.

Kravkatalogets Del III oplister typiske databeskyttelsesretlige minimumskrav efter databeskyttelsesforordningen og -loven til AI-løsninger. Kravene er dog ikke udtømmende, og der vil derfor være behov for at tilpasse kravene samt stille yderligere krav til løsningen i lyset af det konkrete AI-projekt, herunder bl.a. den anvendte teknologi og løsningsmodel (beslutningsstøtte/fuldautomatiske afgørelser), udviklingsmetode (agil udvikling eller vandfaldsmodel) samt resultaterne af de identificerede risici og afvejninger i konsekvensanalysen vedrørende databeskyttelse (**Værktøj 2**) og risikokataloget (**Værktøj 3**). Kravene er således højniveaukrav, der skal nedbrydes i mere specifikke krav til løsningen.

Formuleringen af kravene og dokumentationen heraf i kravkataloget vil skulle opdateres og ændres i takt med, at løsningen ændrer sig under udviklingsprocessen eller efter idriftsættelsen. Kravkataloget er dermed også et dynamisk dokument, som kommunen skal genbesøge løbende.

Kravene vil også skulle tilpasses til den konkrete udbudskontrakt og -form. F.eks. vil der være behov for en ganske præcis og uddybende formulering af kravene til løsningen, hvis kommunen anvender en vandfaldsmodel til udviklingen og udbuddet af løsningen. Anvendes der derimod en agil udviklingsmetode og udbudsform, kan kravene senere i processen nedbrydes i mere præcise krav til løsningen.

I praksis vil det oftest være en fordel at anvende den agile udviklingsmetode ved udbud og udvikling af AI-løsninger. Den agile metode giver mulighed for at definere kravene på et højere funktionelt niveau, og derved sikre bedre konkurrence, da flere AI-løsninger kan komme i spil i udbuddet. Derudover tillader den agile metode mulighed for at udvikle og implementere mindre dele af AI-løsningen ad gangen og derved skalere løsningen gradvis. På denne måde minimeres eventuelle teknologiske og økonomiske risici, der for tiden kan være forbundet med AI-løsningerne.

Ved udbud og anskaffelse af AI-løsninger vil der være behov for at regulere en række almindelige kontraktuelle forhold, f.eks. vederlag og erstatningsansvar. I tilknytning til de immaterialretlige krav i Del IV vil det være hensigtsmæssigt at stille yderligere kontraktuelle krav om overdragelse af data og viden fra leverandøren til kommunen med henblik på at minimere potentiel risiko for leverandørafhængighed, som kan opstå ved brug af forretningskritiske AI-løsninger. I mange kontrakter stilles der desuden krav til CSR. Ved anskaffelse af AI-løsninger kan det være relevant at supplere disse krav med dataetiske krav.

Forud for et udbud er det vigtigt, at kommunen afstemmer kravene til AI-løsningen med leverandørerne på markedet. Dette kan med fordel ske ved brug af markedsdialog, hvor kommunen kan afstemme kravene i forhold til leverandørernes forretningsmodeller og kan afdække leverandørernes vilje og mulighed for at imødekomme kommunen krav. Gennem markedsdialog kan kommunen også sikre, at de stillede krav er proportionelle i forhold til kritikaliteten af AI-løsningen.

# del I: krav til løsningen efter særlovgivningen

Når en kommune ønsker at anvende en AI-løsning indenfor et bestemt område, er det vigtigt, at løsningen er i stand til at opfylde de krav, der følger af særlovgivningen inden for løsningens anvendelsesområde. F.eks. skal løsningen være i stand til at opfylde de relevante regler i beskæftigelseslovgivningens, hvis løsningen skal bistå kommunale sagsbehandlere med beslutningsstøttende faglige vurderinger af lediges kompetencer og jobmuligheder. Reglerne er typisk teknologineutrale, og de regler, der ville gælde for en fysisk sagsbehandler med samme funktion, vil således som det klare udgangspunkt tilsvarende gælde for AI-løsningen.

Angiv nedenfor, hvilken særlovgivning som er relevant for AI-løsningen, og som den skal overholde:

|  |
| --- |
|  |

Angiv nedenfor hvilke krav, som særlovgivningen stiller til AI-løsningen, og hvordan disse overholdes i løsningen:

|  |
| --- |
|  |

# del II: forvaltningsretlige krav til løsningen

AI-løsningen skal også designes til at kunne overholde de almindelige forvaltningsretlige regler, herunder i forvaltningsloven og offentlighedsloven, samt god forvaltningsskik.

Det gælder f.eks. legalitetsprincippet (kravet om hjemmel), officialprincippets krav om tilstrækkelig oplysning af sagen, overholdelse af lighedsgrundsætningen, forbuddet mod skøn under regel og krav til afgørelsers begrundelse. Hvis kommunen ønsker at pålægge borgerne en pligt til at anvende AI-løsningen, skal der være hjemmel i lovgivningen hertil.

AI-løsningen skal også kunne håndtere partsrettigheder for borgerne såsom vejledningspligten, partsrepræsentation, partshøring, aktindsigt, retten til at afgive en udtalelse m.v.

Endelig skal løsningen kunne understøtte de processuelle og ordensmæssige regler, herunder navnlig notat- og journaliseringspligten, arkivpligt m.v.

Du kan læse nærmere om de generelle forvaltningsretlige krav til offentlige it-systemer på Folketingets Ombudsmands hjemmeside her: <http://www.ombudsmanden.dk/myndighedsguiden/specifikke_sagsomraader/generelle_forvaltningsretlige_krav_til_offentlige_it-systemer/>

Angiv nedenfor hvordan de forvaltningsretlige krav overholdes i løsningen:

|  |
| --- |
|  |

# Del III: databeskyttelsesretlige krav til løsningen

Når en kommune anvender en AI-løsning til behandling af personoplysninger, skal løsningen overholde de databeskyttelsesretlige krav efter reglerne i databeskyttelsesforordningen og -loven anvendelse, herunder kunne sikre en effektiv håndtering af databeskyttelsesrisici for de registrerede.

Nedenfor i afsnit 4.1 er oplistet en række væsentlige databeskyttelsesretlige krav, der finder anvendelse, når kommunen anvender en AI-løsning, og som der derfor skal tages højde for ved udviklingen af løsningen.

Når AI-løsningen skal designes, kan der ofte hentes god inspiration til både mulige it-designprincipper og privatlivsfremmende foranstaltninger ved brug af en række data- og procesorienterede designprincipper, der også kan bruges til at nedbryde og tilpasse de ovennævnte databeskyttelsesretlige krav til den konkrete AI-løsning. Disse designprincipper fremgår af afsnit 4.2.

## Databeskyttelsesretlige krav

|  |  |  |  |
| --- | --- | --- | --- |
| **Krav-ID** | **Beskrivelse af krav** | | **Kravets grundlag** |
| **0. Generelle krav om overholdelse af databeskyttelsesretten og overblik over data** | | | |
| DATA-1 | Løsningen skal til enhver tid leve op til gældende ret, herunder særligt opfylde alle relevante krav i databeskyttelsesforordningen og databeskyttelsesloven. Dette indebærer bl.a., at løsningen skal leve op til forordningens grundlæggende principper samt kravet om databeskyttelse gennem design og databeskyttelse gennem standardindstillinger. | | Databeskyttelsesforordningen og databeskyttelsesloven |
| DATA-2 | Løsningen skal til enhver tid kunne håndtere alle typer personoplysninger i overensstemmelse med databeskyttelsesforordningen og databeskyttelsesloven. | | Databeskyttelsesforordningen og databeskyttelsesloven |
| DATA-3 | Løsningen skal understøtte, at der til enhver tid kan dannes et opdateret overblik over, hvilke data, herunder personoplysninger, der anvendes og overføres til tredjeparter i løsningen, herunder 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. | | Databeskyttelsesforordningens artikel 5, stk. 2, artikel 24-25 og 30 |
| **1. Rimelighed og forebyggelse af ulovlig forskelsbehandling** | | | |
| DATA-4 | AI-løsningen skal sikre, at der ikke sker direkte eller indirekte ulovlig forskelsbehandling af fysiske personer på grund af race eller etnisk oprindelse, politisk, religiøs eller filosofisk overbevisning, fagforeningsmæssigt tilhørsforhold, genetisk status eller helbredstilstand eller seksuel orientering.  Med henblik på at understøtte løsningens rimelighed og forebyggelse af ulovlig forskelsbehandling, skal træningen af modellen i AI-løsningen ske ved at anvende passende matematiske eller statistiske procedurer, herunder ved brug af træningsdata, der er så repræsentative som muligt i forhold til de borgere, som AI-løsningen skal anvendes på. | | Databeskyttelsesforordningens artikel 5, stk. 1, litra a |
| DATA-5 | Modellen i løsningen skal udvikles, så den ikke ulovligt tillægger et eller flere bestemte kriterier en uforholdsmæssig stor eller lille vægtning. | | Databeskyttelsesforordningens artikel 5, stk. 1, litra a |
| DATA-6 | Løsningen skal understøtte udskiftning af træningsdata og genoptræning af modellen på ny, hvis tidligere træningsdata har givet anledning til fejl eller ulovlig forskelsbehandling. | | Databeskyttelsesforordningens artikel 5, stk. 1, litra a |
| DATA-7 | *Hvis løsningen har en brugergrænseflade for borgerne:*  Løsningen skal være brugercentreret og designet, så alle i målgruppen kan anvende den – uanset alder, etnicitet, køn, evner og egenskaber. | | Databeskyttelsesforordningens artikel 5, stk. 1, litra a |
| **2. Transparens, forståelighed og systemtransparens** | | | |
| DATA-8 | Løsningens beslutningsprocesser skal være så transparente som muligt for at understøtte princippet om transparens. Løsningen skal designes, så dens beslutningsprocesser kan forklares, herunder hvordan løsningen når frem til (forslag til) beslutninger, logikken og de kriterier/data den lægger vægt på.  Det skal sikres, at et menneske (1) kan forudsige, hvordan systemets output vil ændre sig, hvis input ændrer sig, (2) kan identificere de mest vigtige inputvariable og deres vægt og betydning for afgørelsens resultat, (3) identificere, hvornår outputtet sandsynligvis er forkert. | | Databeskyttelsesforordningens artikel 5, stk. 1, litra a, artikel 13-15 og artikel 22 |
| DATA-9 | Løsningen skal understøtte sporbarhed af løsningens beslutninger. Som følge heraf skal de metoder, der er blevet anvendt til design og udvikling af løsningens algoritme dokumenteres.  Hvis der er tale om et regelbaseret system, bør programmeringsmetoden eller den måde, systemet er bygget på, dokumenteres. Hvis der er tale om et læringsbaseret AI-system, bør der ske dokumentation af metoden til oplæring af algoritmen, herunder hvilke inputdata der er indsamlet og udvalgt, og hvordan dette er sket. | | Databeskyttelsesforordningens artikel 5, stk. 1, litra a |
| DATA-10 | Inden endelig godkendelse og produktionssætning og ibrugtagning af AI-løsningen skal leverandøren overdrage systemdokumentation for løsningen samt (hvis relevant) udførlige driftsvejledninger til kommunen. | | Databeskyttelsesforordningens artikel 5, stk. 2, og artikel 24, stk. 1 |
| DATA-11 | *Hvis løsningen er baseret på en dynamisk (læringsbaseret) model:*  Hvis ændringer i løsningens datagrundlag giver anledning til nye vægtninger eller anderledes afvejninger af kriterier, skal løsningen være i stand til at gøre sagsbehandlere opmærksomme herpå, f.eks. ved notifikationer ved udsving af en bestemt størrelse. | | Databeskyttelsesforordningens artikel 5, stk. 1, litra a |
| **3. Formålsbegrænsning** | | | |
| DATA-12 | Løsningen skal udvikles således, at der alene indsamles personoplysninger til udtrykkeligt angivne og legitime formål. | | Databeskyttelsesforordningens artikel 5, stk. 1, litra b, og databeskyttelseslovens § 5, stk. 1 |
| DATA-13 | Løsningen skal understøtte, at indsamlede personoplysninger ikke bliver viderebehandlet til formål, der er uforenelige med indsamlingsformålet. | | Databeskyttelsesforordningens artikel 5, stk. 1, litra b, og databeskyttelseslovens § 5, stk. 1 |
| DATA-14 | Løsningen skal understøtte mulighed for en klar opdeling af behandling af personoplysninger i miljøer for udvikling og anvendelse af modellen/systemet (data governance). | | Databeskyttelsesforordningens artikel 5, stk. 1, litra b, og databeskyttelseslovens § 5, stk. 1 |
| **4. Dataminimering og opbevaringsbegrænsning** | | | |
| DATA-15 | Løsningen skal understøtte overholdelse af princippet om dataminimering ved udvikling (træning) og anvendelse af løsningen. Som følge heraf må AI-løsningen ikke indsamle eller behandle flere personoplysninger, end hvad der er tilstrækkeligt, relevant og nødvendigt i lyset af løsningens formål. Løsningen skal understøtte, at der kan ske en periodisk evaluering af proportionaliteten i databehandlingen med henblik på at eliminere datakilder, der ikke længere er nødvendige i lyset af formålet. | | Databeskyttelsesforordningens artikel 5, stk. 1, litra c |
| DATA-16 | Løsningen skal understøtte brug af pseudonymisering, anonymisering og aggregering i videst muligt omfang, så systemet til enhver tid behandler så få personoplysninger som muligt i lyset af løsningens formål. | | Databeskyttelsesforordningens artikel 5, stk. 1, litra c |
| DATA-17 | Ved terminaladgang eller løbende abonnement af oplysninger fra eksterne registre, skal løsningen understøtte, at der ved indsamling eller videregivelse ikke henholdsvis indsamles eller videregives flere oplysninger end nødvendigt. | | Databeskyttelsesforordningens artikel 5, stk. 1, litra c |
| DATA-18 | Løsningen skal understøtte sletning af træningsdata og testdata, så snart de ikke længere er relevante, herunder i udviklingsmiljøer. | | Databeskyttelsesforordningens artikel 5, stk. 1, litra c |
| DATA-19 | Løsningen skal understøtte, at oplysninger kan slettes eller anonymiseres effektivt og uigenkaldeligt i løsningen, herunder i udviklings- og testmiljøer, efter en rimelig og på forhånd fastsat periode samt ved forlangende. | | Databeskyttelsesforordningens artikel 5, stk. 1, litra e |
| DATA-20 | *Hvis løsningen er baseret på en dynamisk (læringsbaseret) model:*  Løsningen skal udgøre en stabil og pålidelig beslutningsmodel, hvorfor løbende sletning af personoplysninger ikke må forårsage markante praksisændringer for løsningens beslutninger. | | Databeskyttelsesforordningens artikel 5, stk. 1, litra a og e |
| **5. Datakvalitet** | | | |
| DATA-21 | Med henblik på at overholde princippet om rigtighed skal løsningen navnlig sikre, at faktorer, der resulterer i unøjagtige personoplysninger, bliver rettet, og at risikoen for fejl minimeres. Løsningen skal indeholde en beskrivelse af, hvordan alle personoplysninger, der anvendes til træning, test og anvendelse af AI-systemet, er så korrekte, relevante, repræsentative, komplette og ajourførte som muligt. | | Databeskyttelsesforordningens artikel 5, stk. 1, litra d |
| DATA-22 | Løsningen skal understøtte ændring, berigtigelse og ajourføring af registrerede personoplysninger, herunder både på kommunens eget initiativ eller ved henvendelse herom fra den registrerede selv. | | Databeskyttelsesforordningens artikel 5, stk. 1, litra d |
| DATA-23 | Løsningen skal understøtte et overblik over de kriterier og deres vægtning, der indgår i modellen. Det skal være muligt at få indsigt i modellens nøjagtighed og træfsikkerhed samt at kunne beskrive dens begrænsninger. | | Databeskyttelsesforordningens artikel 5, stk. 1, litra d |
| **6. Registreredes rettigheder** | | | |
| DATA-24 | Løsningen skal understøtte, at brugerne kan udøve deres rettigheder efter databeskyttelsesforordningen. 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. | | Databeskyttelsesforordningens kapitel III |
| **7. Fuldautomatiske afgørelser og profilering** | | | |
| DATA-25 | Løsningen skal understøtte, at der kan foretages en løbende overvågning og mulighed for menneskelig overvågning og indgriben før/efter AI-løsningen har truffet en afgørelse. Ved den manuelle kontrol med outputtet af systemet skal der være adgang til relevant viden om, hvorvidt den forudsatte kvalitet af outputtet er tilstrækkelig og i overensstemmelse med fastsatte kvalitetskrav, f.eks. at der er en kvalitetsscore af outputtet tilgængelig for brugeren, der kan forklares. | | Databeskyttelsesforordningens artikel 5, stk. 2, artikel 22 og 24 |
| DATA-26 | Løsningen skal understøtte, at der kan foretages en klar og dokumenteret grænsedragning mellem fuldautomatiske afgørelser og beslutningsstøtte i de situationer, hvor der anvendes en kombination af de to. | | Databeskyttelsesforordningens artikel 5, stk. 2, artikel 22 og 24 |
| DATA-27 | Hvis AI-løsningen indebærer fuldautomatiske afgørelser, herunder ved brug af profilering, skal løsningen understøtte, at den registreredes kan oplyses herom samt modtage meningsfulde oplysninger om logikken heri samt betydningen og de forventede konsekvenser af en sådan behandling for den registrerede. Den registrerede har også ret til indsigt i disse oplysninger.  I stedet for at komme med en kompleks matematisk forklaring på, hvordan algoritmer eller maskinlæring fungerer, bør den dataansvarlige overveje at anvende klare og omfattende metoder til at give oplysningerne til den registrerede, f.eks. ved at oplyse om:   * De kategorier af oplysninger, der er eller vil blive anvendt i forbindelse med profileringen eller beslutningstagningen * hvorfor disse kategorier anses for at være relevante * hvordan en profil, der anvendes i forbindelse med automatiske afgørelser, er opbygget, herunder eventuelle statistiske oplysninger, der er anvendt i analysen * hvorfor denne profil er relevant i forbindelse med automatiske afgørelser * hvordan den anvendes til en afgørelse vedrørende den registrerede. | | Databeskyttelsesforordningens artikel 5, stk. 1, litra a, artikel 12-15 og 22 |
| DATA-28 | Løsningen skal understøtte muligheden for menneskelig overvågning og indgriben før/efter løsningen har truffet en afgørelse. | | Databeskyttelsesforordningens artikel 22 |
| **8. Robusthed og sikkerhed** | | | |
| For identifikation og implementering af krav vedrørende AI-løsningens robusthed og sikkerhed henvises til følgende yderligere vejledning:   * KL’s materiale vedrørende risikostyring på KL og KOMBIT’s videncenter, som kan findes her: <https://videncenter.kl.dk/viden-og-vaerktoejer/informationssikkerhed-og-gdpr/risikostyring/> eller egne vejledninger. * Digitaliseringsstyrelsen, Erhvervsstyrelsen og Center for Cybersikkerhed: Vejledning: Tiltag til at sikre brugen af kunstig intelligens, januar 2020, som kan findes her: <https://digst.dk/nyheder/nyhedsarkiv/2020/februar/vejledning-om-fokus-paa-sikkerhed-ved-brug-af-kunstig-intelligens-i-praksis/> * ISO/IEC 27001:2013, Anneks A, som kan findes her (kræver licensbetaling): <https://www.iso.org/standard/54534.html> * ISO/IEC 29134:2017 og ISO/IEC 29151:2017, der i katalogform beskriver flere af de mulige sikkerhedsforanstaltninger, der kan benyttes. Standarderne kan findes her (kræver licensbetaling): <https://www.iso.org/standard/62289.html> og her: <https://www.iso.org/standard/62726.html> | | | |
| **9. Governance og ansvarlighed** | | | |
| DATA-29 | | Løsningen skal understøtte dokumentation, herunder versionering af løsningen, af valg og ændringer af AI-løsningen, så kommunen altid kan dokumentere valg og fravalg under udvikling, drift og opdatering af systemet samt begrundelserne herfor. | Databeskyttelsesforordningens artikel 5, stk. 2, og artikel 24, stk. 1 |
| DATA-30 | | Løsningen skal understøtte, at kommunen selv eller en tredjepart kan gennemføre en algoritmisk audit af AI-systemet, modellen eller kildekoden. Dvs. en audit for at påvise, at systemet rent faktisk fungerer efter hensigten og ikke giver diskriminerende, fejlagtige eller uberettigede resultater. | Databeskyttelsesforordningens artikel 5, stk. 2, og artikel 24, stk. 1 |

## Designprincipper vedrørende databeskyttelse

Når AI-løsningen skal designes, kan der ofte hentes god inspiration til både mulige it-designprincipper og privatlivsfremmende foranstaltninger ved brug af følgende 5 *dataorienterede* designprincipper, der også kan bruges til at nedbryde og tilpasse de ovennævnte databeskyttelsesretlige krav til den konkrete AI-løsning.[[1]](#footnote-1)

1. *Minimér og begræns*: Mængden af personoplysninger der indsamles og behandles, skal være begrænset til, hvad der er lovligt og strengt nødvendigt (”select before you collect”). Derudover skal oplysningerne slettes så snart, de ikke længere er nødvendige for behandlingens formål.
2. *Skjul og beskyt*: Personoplysninger og deres interne sammenhænge skal hverken kommunikeres, behandles eller opbevares frit fremme. Dette designprincip kan f.eks. opfyldes ved brug af pseudonymisering, kryptering og aggregering af personoplysningerne.
3. *Separér*: Ved at adskille forskellige behandlinger af personoplysninger om samme person, mindskes muligheden for at oprette komplette profiler af vedkommende. Dette designprincip kan f.eks. opfyldes ved at gemme personoplysningerne i separate databaser, enheder og områder til forskellige formål. Dette designprincip understøtter også formålsbestemthed, idet personoplysninger til forskellige formål – f.eks. personoplysninger til brug for udvikling og anvendelse af AI-løsningen – holdes adskilt.
4. *Aggregér*: Dette designprincip handler om at indsamle og behandle personoplysninger i så aggregeret form som muligt. Personoplysningerne skal være så begrænsede, ikke-detaljerede, ikke-fortrolige og ikke-følsomme som muligt – med respekt for behandlingens formål.
5. *Databeskyttelse gennem standardindstillinger*: AI-løsningen skal som udgangspunkt være konfigureret med de mest privatlivsvenlige indstillinger muligt, herunder navnlig at der ikke indsamles og opbevares flere personoplysninger end nødvendigt for behandlingen. Brugeren af løsningen skal dermed aktivt vælge at indstille mindre privatlivsvenligt.

Beskriv nedenfor, hvordan ovenstående dataorienterede designprincipper er blevet implementeret i AI-løsningens design:

|  |
| --- |
|  |

Udover de dataorienterede designprincipper kan følgende 4 *procesorienterede* designprincipper ligeledes inddrages ved udformningen af AI-løsningens design[[2]](#footnote-2):

1. *Informér*: AI-løsningen designes, så den registrerede bliver tilstrækkeligt informeret om, hvordan løsningen fungerer samt hvordan vedkommendes personoplysninger bliver behandlet. Informationen tilpasses til brugergruppen. Hvis AI-løsningen foretager profilering eller træffer automatiske afgørelser, skal den registrerede informeres om, hvordan dette foregår, samt konsekvenserne for den registrerede.
2. *Kontrollér*: Den registrerede har ret til at kontrollere egne personoplysninger. Derudover har den registrerede ret til at kræve manuel behandling i tilfælde, hvor AI-løsningen anvendes til at træffe fuldautomatiske afgørelser. AI-løsningen skal som konsekvens heraf være indrettet, så den registrerede nemt er i stand til at udøve disse rettigheder.
3. *Håndhæv:* AI-løsningen skal være designet, så den understøtter dokumentation af, hvordan den sikrer overholdelse databeskyttelsesreglerne (princippet om ansvarlighed). Dokumentationen skal i denne forbindelse dække ansvarsforhold samt hvordan databeskyttelsesforordningen håndhæves, og den skal være tilgængelig ved revisioner eller inspektioner af AI-løsningen.
4. *Demonstrér*: AI-løsningen skal være designet og udviklet, så den dataansvarlige kan dokumentere og demonstrere, hvordan kravene i databeskyttelsesforordningen er blevet implementeret. Eksempelvis kan den dataansvarlige fremlægge dokumentation for udførte tests, rapporter fra sikkerhedsrevisioner, sårbarhedsscanninger og rapporter om håndtering af sikkerhedsbrud m.v.

Beskriv nedenfor, hvordan ovenstående procesorienterede designprincipper er blevet implementeret i AI-løsningens design:

|  |
| --- |
|  |

# del IV: Væsentlige immaterialretlige krav (rettighedsbestemmelser)

Hvis en kommune får **specialudviklet** et AI-system, bør kommunen overveje, hvilke bestemmelser aftalen med leverandøren skal indeholde i forhold til det materiale, som kan være beskyttet af immaterielle rettigheder. Dette materiale kan opdeles i følgende:

1. Den **software**, der indgår i systemet,
2. de **data**, der benyttes i systemet, og
3. de **resultater**, der kommer ud af at benytte systemet.

På den baggrund gives nedenfor eksempler på rettighedsbestemmelser, som kommunen kan kræve indsat i aftalen med leverandøren.

Hvis kommunen – i stedet for at udvikle et særligt AI-system – ønsker at benytte et **standardiseret** AI-system, vil kommunen typisk være nødt til at acceptere udbyderens standardaftale herom. I en sådan situation vil det næppe være muligt for kommunen at stille krav til aftalens rettighedsbestemmelser.

## Rettighedsbestemmelser til den software, der indgår i AI-systemet

|  |  |  |
| --- | --- | --- |
| **Rettighedsbestemmelser til den software, der indgår i AI-systemet** | | |
| Efterhånden som leverandøren udvikler den software, der indgår i AI-systemet, opstår oftest en eksklusiv immaterialret til softwaren hos leverandøren. Dette gælder også, selvom kommunen har fået ideen til systemet og bestemmer, hvilke opgaver softwaren skal kunne løse.  For at sikre sin og eventuelt andres ret til at benytte softwaren bør kommunen derfor stille krav om rettigheder til softwaren i aftalen med leverandøren.  Overordnet skelnes mellem selve den **eksklusive immaterialret** og en **simpel brugsret**. | | |
| Krav-ID | Kravformulering | Beskrivelse af kravet |
| IP-1 | I det omfang software, der indgår i AI-systemet, er beskyttet af immaterielle rettigheder, herunder ophavs-, design- og patentrettigheder samt rettigheder efter markedsføringsloven, erhverver kommunen samtlige rettigheder til denne software.  Kommunen kan frit helt eller delvist overdrage rettighederne til og ændre softwaren og i øvrigt udøve enhver rettighed som ejer.  Leverandøren garanterer, at tredjeparts eventuelle rettigheder til softwaren er fuldt klareret, således at kommunen erhverver samtlige rettigheder til softwaren som anført i dette punkt. Leverandøren skal skadesløsholde kommunen for ethvert krav, der måtte opstå som følge af, at tredjeparts rettigheder ikke er fuldt klareret.  Leverandøren skal stille de eventuelt nødvendige redskaber og oplysninger, fx kildekode og dokumentation, til rådighed for kommunen, således at kommunen kan udnytte sine rettigheder i overensstemmelse med dette punkt. | Kommunen ønsker at erhverve den eksklusive immaterialret til softwaren  Erhvervelse af selve immaterialretten indebærer den fordel, at kommunen får ret til at råde helt frit over softwaren. Fx får kommunen ret til selv at vedligeholde og videreudvikle softwaren uafhængigt af leverandøren, og kommunen får ret til at stille softwaren til rådighed for andre kommuner.  Kommuner, som ikke skal konkurrere på noget marked, vil typisk kun have interesse i at erhverve selve immaterialretten i tilfælde, hvor det er yderst vigtigt at kunne udnytte softwaren helt frit, men hvor det samtidig ikke på forhånd præcist kan indkredses, hvad softwaren skal bruges til. |
| IP-2 | Kommunen tildeler leverandøren en brugsret til softwaren, således at Leverandøren tidsubegrænset kan benytte softwaren på enhver måde, der ikke hindrer eller hæmmer kommunens benyttelse af softwaren. | Kommunen ønsker at tildele leverandøren en simpel brugsret til softwaren  Erhvervelsen af selve immaterialretten vil typisk være relativ dyr. Det skyldes, at leverandøren ved overdragelse af selve immaterialretten til én kunde ikke længere frit kan udnytte softwaren i forhold til andre kunder. En gylden middelvej vil eventuelt kunne være, at kommunen tildeler leverandøren en brugsret. |
| IP-3 | I det omfang software, der indgår i AI-systemet, er beskyttet af immaterielle rettigheder, herunder ophavs-, design- og patentrettigheder samt rettigheder efter markedsføringsloven, erhverver kommunen brugsret til denne software.  Kommunens brugsret til softwaren er royalty-fri og ikke-eksklusiv. Brugsretten er tidsmæssigt, geografisk og kvantitativt ubegrænset. Kvalitativt omfatter brugsretten enhver brug internt og eksternt i forbindelse med kommunens virksomhed, herunder i forbindelse med kommunens udbud af ydelser. Brugsretten omfatter i den forbindelse også de rettigheder for tredjemand, der er nødvendige for, at kommunen kan modtage tilbud fra tredjemand.  Kommunen har desuden ret til at foretage ændringer af softwaren, herunder i forbindelse med vedligeholdelse og videreudvikling.  Endelig har kommunen ret til at lade tredjemand, der bistår kommunen internt og eksternt i forbindelse med kommunens virksomhed, benytte softwaren og foretage ændringer på samme måde som kommunen, fx ved vedligeholdelse og videreudvikling på kommunens vegne.  Leverandøren garanterer, at tredjeparts eventuelle rettigheder til softwaren er fuldt klareret, således at kommunen erhverver samtlige rettigheder til softwaren som anført i dette punkt. Leverandøren skal skadesløsholde kommunen for ethvert krav, der måtte opstå som følge af, at tredjeparts rettigheder ikke er fuldt klareret.  Leverandøren skal stille de eventuelt nødvendige redskaber og oplysninger, fx kildekode og dokumentation, til rådighed for kommunen, således at kommunen kan udnytte sine rettigheder i overensstemmelse med dette punkt. | Kommunen ønsker at erhverve en brugsret til AI-løsningen  Erhvervelse af en brugsret indebærer typisk den fordel, at kommunen kun skal betale for sin specifikke brug af softwaren.  De overordnede ulemper er *dels*, at kommunen risikerer at blive afhængig af leverandøren, hvis leverandøren er den eneste, som kan levere vedligeholdelse og videreudvikling af softwaren samt fornyelse af brugsretten, *dels* at kommunen kun får den brugsret, der er specifikt beskrevet i aftalen.  Kommunen bør derfor som hovedregel stille krav om en meget bredt specificeret brugsret, som den i eksemplet. |

## Rettighedsbestemmelser til de data, der benyttes i AI-løsningen

|  |  |  |
| --- | --- | --- |
| **Rettighedsbestemmelse til de data, der benyttes i AI-løsningen** | | |
| Enkeltstående data er ikke i sig selv beskyttet af nogen immaterialret. Hvis data samles og systematiseres i en database, kan der imidlertid opstå en immaterialretlig beskyttelse til databasen.  For at sikre sin og eventuelt andres ret til at benytte de data, der benyttes i AI-systemet, bør kommunen derfor stille krav om rettigheder hertil.  Det forudsættes, at alle data, der benyttes i AI-systemet, oprindeligt stammer fra kommunen og udelukkende bør kunne benyttes af leverandøren i forbindelse med opfyldelse af aftalen med kommunen.  Kommunen bør derfor som hovedregel stille krav om bevarelse/erhvervelse af selve immaterialretten til de data, der benyttes i AI-systemet. | | |
| Krav-ID | Kravformulering | Beskrivelse af kravet |
| IP-4 | Kommunen bevarer enhver rettighed til data, som kommunen enten havde før aftalens indgåelse eller senere erhverver under andre kontraktforhold. Kommunen erhverver desuden enhver rettighed til data, som leverandøren frembringer eller leverer, eller som i øvrigt opstår i forbindelse med aftalens opfyldelse.  Disse data kaldes herefter kommunens data. Kommunens data omfatter dog ikke data, som kun er relevant for leverandøren, fx data vedrørende leverandørens medarbejdere.  Leverandøren må udelukkende anvende kommunens data i forbindelse med aftalens opfyldelse. | Eksempel på bestemmelse om erhvervelse af selve immaterialretten til AI-løsningens data |

## Rettighedsbestemmelser til de resultater, der kommer ud af at benytte AI-løsningen

|  |  |  |
| --- | --- | --- |
| **Rettighedsbestemmelse til de resultater, der kommer ud af at benytte AI-løsningen** | | |
| Det er omdiskuteret, om de resultater, der kommer ud af at benytte et AI-system, fx (dele af) afgørelser eller rapporter, er immaterialretligt beskyttet.  Formentlig er det ikke tilfældet, men for under alle omstændigheder at sikre sin og eventuelt andres ret til at benytte disse resultater, bør kommunen stille krav om rettigheder hertil.  Det forudsættes, at ethvert resultat, som AI-systemet genererer, kun er relevant for kommunen samt kommunens borgere og samarbejdspartnere mv., og udelukkende bør kunne benyttes af leverandøren i forbindelse med opfyldelse af aftalen med kommunen.    Kommunen bør derfor som hovedregel stille krav om erhvervelse af selve immaterialretten til de resultater, der kommer ud af at benytte AI-systemet. | | |
| Krav-ID | Kravformulering | Beskrivelse af kravet |
| IP-5 | I det omfang de resultater, fx [*indsæt typeeksemplet på de resultater, som AI-systemet genererer, fx (dele af) afgørelser eller rapporter*], der kommer ud af at benytte AI-systemet, er beskyttet af immaterielle rettigheder, erhverver kommunen samtlige rettigheder hertil.  Kommunen kan frit helt eller delvist overdrage rettighederne til samt ændre resultaterne og i øvrigt udøve enhver rettighed som ejer.  Leverandøren garanterer, at tredjeparts eventuelle rettigheder til resultaterne er fuldt klareret, således at kommunen erhverver samtlige rettigheder til resultaterne som anført i dette punkt. Leverandøren skal skadesløsholde kommunen for ethvert krav, der måtte opstå som følge af, at tredjeparts rettigheder ikke er fuldt klareret.  Leverandøren skal stille de eventuelt nødvendige redskaber og oplysninger, fx datagrundlag og beregningsmetoder til rådighed for kommunen, således at kommunen kan udnytte sine rettigheder i overensstemmelse med dette punkt.  Leverandøren må udelukkende anvende de resultater, der kommer ud af at benytte AI-systemet i forbindelse med aftalens opfyldelse. | Eksempel på bestemmelse om erhvervelse af selve immaterialretten til resultater |

1. Se Datatilsynet, Justitsministeriet og Digitaliseringsstyrelsen: Vejledning - Behandlingssikkerhed og databeskyttelse gennem design og standardindstillinger, juni 2018, s. 25 f og 30, smh. det norske datatilsyn: Software development with Data Protection by Design and by Default, version af 28. november 2017 [↑](#footnote-ref-1)
2. Se ovenfor anførte sted [↑](#footnote-ref-2)