|  |
| --- |
| **Juridisk værktøjskasse for Ansvarlig AI****Værktøj nr. 1**Tjeklister til centrale aktiviteter i udviklingen af AI-løsningen |

 

Indholdsfortegnelse

[Indledning 3](#_Toc43910950)

[1. Governance og projektetablering 5](#_Toc43910951)

[2. Projektopstart 6](#_Toc43910952)

[3. Kravsætning 8](#_Toc43910953)

[4. Design 9](#_Toc43910954)

[5. Indsamling af data, træning og validering af modellen 10](#_Toc43910955)

[6. Konstruktion af AI-løsningen 12](#_Toc43910956)

[7. Test af AI-løsningen 12](#_Toc43910957)

[8. Release af AI-løsningen 14](#_Toc43910958)

[9. Løbende kontrol i drift 15](#_Toc43910959)

# Indledning

Dette værktøj indeholder en række tjeklister for, hvad man skal være særligt opmærksom på ved udvikling og anvendelse af AI-løsninger for dels at kunne understøtte håndteringen af risici vedrørende databeskyttelse, dels overholde de retlige krav til løsningen efter navnlig databeskyttelsesforordningen og -loven.

Værktøjet omfatter tjeklister for hver enkelt central aktivitet i udviklingen af AI-løsningen i løbet af hele løsningens livscyklus – fra opstart og udvikling til idriftsættelse og løbende kontrol – som følger:

*Figur 1. Centrale aktiviteter i udviklingen af AI-løsningen*



Ovennævnte aktiviteter skal ikke ses som en fast fasemodel, som kommunerne slavisk skal følge, men netop som centrale aktiviteter, der kan tilpasses og tilrettelægges i kommunernes allerede etablerede projekt- og udviklingsmodeller. Det er også vigtigt at bemærke, at nogle kommuner udvikler ved brug af en agil udviklingsmetode med iterative processer, hvorimod andre bruger en vandfaldsmodel, hvor kravene til løsningen fastsættes relativt udførligt tidligt i processen, hvorefter den udvikles og idriftsættes. En sådan tilpasning af aktiviteterne i dette værktøj til kommunens eksisterende setup vil derfor ofte være nødvendig.

# Governance og projektetablering

Denne aktivitet befinder sig tidsmæssigt forud for opstart af projekt om udvikling af den konkrete AI-løsning. Formålet med aktiviteten er at etablere et godt og solidt fundament for udvikling og anvendelse af AI-løsninger gennem klare ansvars- og rollefordelinger (governance).

Der skal være tale om implementering af dokumenterede retningslinjer, beslutningsgange og procedurer, der sikrer ansvaret og ansvarligheden for AI-systemet og dets resultater i hele systemets livscyklus. Disse mekanismer skal klart regulere, hvornår ledelsen skal godkende centrale milepæle, herunder beslutning om opstart, udvikling af modellen, idriftsættelse og revision samt centrale performancekrav.

Kommunen vil normalt allerede have en eksisterende governancestruktur og projektmodel for gennemførelse af projekter, herunder ved brug af agile udviklingsmodeller. Udviklingen og anvendelsen af AI-løsningen bør som udgangspunkt følge disse eksisterende processer, herunder for inddragelse af databeskyttelsesrådgiveren og it-sikkerhedsansvarlige. Brugen af AI kan dog introducere nye risici, ligesom udvikling og anvendelse af AI-løsningen kan medføre nye processer. Kommunen skal derfor overveje, om de eksisterende forretningsgange og ansvarsfordelinger skal tilpasses til den nye kontekst.

Målgruppen for denne aktivitet er alle relevante medarbejdere, der beskæftiger sig med udvikling af AI-løsninger i kommunen, dvs. projektledere, udviklere, IT-arkitekter, digitaliseringskonsulenter, systemejere, sikkerheds- og databeskyttelsesansvarlige, herunder databeskyttelsesrådgivere (DPO’ere), dataanalytikere (data scientists) og personer med domænekendskab (faglige fyrtårne / erfarne sagsbehandlere). Det vil også ofte være relevant at inddrage kommunens borgerrådgiver.

Målet er, at alle involverede har en overordnet forståelse af den ansvars- og rollefordeling, der gælder ved udviklingen af en AI-løsning.

*Afkryds nedenfor de handlinger, som er blevet gennemført*

|  |  |
| --- | --- |
| [ ]  | Der er fastlagt en klar og dokumenterbar organisationsstruktur for udviklingen og anvendelsen af AI-løsninger med fokus på hvem, der har ansvar for hvilke aspekter af udviklingen, samt for ledelsesgodkendelse af centrale skridt og milepæle og performancekrav.  |
| [ ]  | Der er fastlagt en klar og dokumenterbar organisationsstruktur for ledelsesgodkendelse af centrale skridt, milepæle og performancekrav.  |

Bemærkninger til ovenstående punkter:

|  |
| --- |
|  |

# Projektopstart

Denne aktivitet har til formål at beskrive formålet med projektet, dvs. hvad kommunen ønsker at opnå med projektet, f.eks. en løsning til bedre understøttelse af målrettede beskæftigelsesindsatser til ledige borgere, samt hvorfor opgaven bedst kan løses med brug af AI.

Derudover skal aktiviteten understøtte, at det nødvendige faglige grundlag foreligger i forhold til udviklingen af AI-løsningen. De relevante medarbejdere, der skal være med til at udvikle AI-løsningen skal være oplært i dels de databeskyttelsesretlige regler, dels de regler i særlovgivningen, som gælder på det område, som AI-løsningen vedrører. Alternativt skal der inddrages juridisk ekspertise i form af fageksperter.

Alt afhængig af kommunens projektmodel vil der ofte blive udarbejdet et projektgrundlag i form af en projektbeskrivelse eller formulering af en egentlig business case samt en eller flere centrale use-cases for den sagsbehandling, som løsningen skal håndtere. Der vil også ofte blive opstillet nogle succeskriterier for det forventede udbytte af løsningen, så det kan vurderes, om AI-løsningen vil være rentabel.

Formålet og målsætningerne med AI-løsningen og beskrivelsen af de scenarier og sager, som AI-løsningen skal kunne håndtere, danner herefter udgangspunkt for den videre udvikling af AI-løsningen. Derudover vil der typisk skulle tages stilling til valg af en AI-model, som skønnes bedst egnet til opgaven.

Når det skal vurderes, om brug af AI er den bedste løsning – samt ved valg af AI-model – er det vigtigt at have et indgående kendskab til, hvilke sager og problemer systemet skal løse. Derudover er det også relevant så tidligt som muligt i projektet at få et overblik over, hvilke data man har til rådighed, at disse data har den fornødne kvalitet, samt at kommunen retligt kan bruge disse data til træning og anvendelse i løsningen, jf. nærmere herom i aktivitet nr. 5 nedenfor.

Det er også ofte på dette stadie i processen, at kommunen tager stilling til og afklarer, om AI-løsningen skal egenudvikles af kommunen selv eller købes enten som standard eller skræddersyet løsning af eksterne leverandører. Det vil her normalt være afgørende for kommunens beslutning om egenudvikling, hvorvidt kommunen vurderer, at kommunen har kompetencerne til udvikling, drift og vedligehold af løsningen selv.

Målgruppen for denne aktivitet er primært projektlederen samt personer, der kender de tilgængelige data (data scientists) samt personer med domænekendskab, dvs. faglige specialister, der kender forvaltningsområdet og det problem, systemet skal løse. Det er også relevant at inddrage kommunens databeskyttelsesrådgiver fra start. Ledelsen/styregruppe vil typisk skulle godkende projektoplæg og dets succeskriterier.

*Afkryds nedenfor de handlinger, som er blevet gennemført*

|  |  |
| --- | --- |
| [ ]  | Er det klart beskrevet og dokumenteret, hvad formålet med AI-løsningen er, samt hvorfor opgaven bedst kan løses ved brug af AI, og er dette tydeligt kommunikeret, så alle involverede forstår det? Dette kan være med til at understøtte overholdelse af princippet om formålsbegrænsning. |
| [ ]  | Har I gjort jer klart – og eventuelt formuleret relevante use-cases for – hvilke sagstyper, processer, sagsbehandling og øvrige forretningsmæssige behov, som AI-løsningen skal kunne håndtere? |
| [ ]  | Har I overvejet, hvilke data I har behov for, dataenes kvalitet og at dataene retligt må anvendes til udvikling og anvendelse i løsningen? |
| [ ]  | Har I dokumenteret valget af model, dvs. hvilken model der skønnes bedst egnet til at udføre opgaven (f.eks. superviseret machine learning), og om modellen skal være en dynamisk eller statisk model, samt om der skal være tale om et system baseret på beslutningsstøtte eller fuldautomatiske afgørelser? Valg af model og system skal så vidt muligt beskrives, herunder begrænsninger, og det skal dokumenteres, når der sker ændringer, således at modellens og systemets historik er sikret.  |
| [ ]  | Har I inddraget kommunens databeskyttelsesrådgiver som sparringspartner fra start i processen? |
| [ ]  | De ansatte, der skal være med til udviklingen af AI-løsningen, er blevet undervist i databeskyttelsesforordningens og -lovens krav, så de har en grundlæggende forståelse for navnlig de grundlæggende behandlingsprincipper, behandlingssikkerhed, kravet om indbygget databeskyttelse og databeskyttelse gennem standardindstillinger, konsekvensanalyse vedrørende databeskyttelse samt kravene til brug af automatiske afgørelser.  |
| [ ]  | De ansatte, der skal være med til udviklingen af AI-løsningen, er blevet undervist i de krav, der følger af relevant særlovgivning, standarder og interne regler og krav på området. Alternativt er der inddraget juridisk ekspertise i form af fageksperter. |
| [ ]  | De ansatte, der skal være med til udviklingen af AI-løsningen, er blevet introduceret til denne værktøjskasse. |

Bemærkninger til ovenstående punkter:

|  |
| --- |
|  |

# Kravsætning

I denne aktivitet vil kommunen formulere de forretningsmæssige behov til løsningen, dvs. hvad løsningen konkret skal kunne for at leve op til formålet med løsningen (forretningsmæssige krav).

I løbet af denne aktivitet skal det også afklares, hvilke krav AI-løsningen skal kunne leve op til for at opfylde relevant lovgivning og imødegå databeskyttelsesmæssige risici for de registrerede (borgerne). Det er vigtigt at få afdækket disse krav til løsningen så tidligt som muligt, så udviklerne af AI-løsningen har mulighed for at bygge og tilpasse løsningen med disse krav indtænkt fra start. På denne måde reduceres risikoen for senere tilbageløb og fordyrende ændringer, fordi løsningen ikke lever op til kravene.

Målgruppen for denne aktivitet består navnlig af kravstillere, produktejere, udviklere, it-arkitekter og data scientists. Databeskyttelsesrådgiveren og it-sikkerhedsrådgiveren skal også inddrages under denne aktivitet for at bidrage til at nedbryde de juridiske databeskyttelsesretlige krav til mere konkrete krav til løsningen. Tilsvarende vil det ofte være relevant at inddrage fageksperter, der har juridiske kompetencer inden for den særlovgivning og område, som løsningen vedrører.

*Afkryds nedenfor de handlinger, som er blevet gennemført*

|  |  |
| --- | --- |
| [ ]  | Har I kortlagt og undersøgt relevant særlovgivning for, hvilke krav den stiller til de sager, som AI-løsningen skal håndtere, og hvordan særlovgivningen overholdes i løsningen og dokumenteret disse krav? (Brug kravkataloget i **Værktøj nr. 4**) |
| [ ]  | Har I kortlagt og undersøgt den tværgående og generelle lovgivning for, hvilke krav den stiller til AI-løsningen, og hvordan kravene overholdes ved udvikling og anvendelse af løsningen og dokumenteret dette? Omfattet er navnlig forvaltningsretten, herunder forvaltningsloven og offentlighedsloven, samt antidiskriminationslovgivning m.v. (Brug kravkataloget i **Værktøj nr. 4**)  |
| [ ]  | Har I foretaget en konsekvensanalyse vedrørende databeskyttelse for AI-løsningens behandlinger af personoplysninger for at identificere og håndtere risici og fastsætte krav til løsningen? (Brug **Værktøj nr. 2 og 3**) |
| [ ]  | Har I afklaret, om udviklingen og anvendelsen af AI-løsningen sker i overensstemmelse med kommunens allerede eksisterende retningslinjer for f.eks. it-sikkerhed, risikostyring og øvrige interne regler m.v., samt relevante standarder på området, adfærdskodekser eller dataetiske regelsæt? |

Bemærkninger til ovenstående punkter:

|  |
| --- |
|  |

# Design

I løbet af denne aktivitet skal det sikres, at AI-løsningen bliver designet, så den er i stand til at opfylde alle de relevante krav, der er konstateret under aktiviteten ”kravsætning”. Derudover skal øvrige designkrav identificeres, så it-arkitekterne kan indtænke disse i designet af AI-løsningen.

Målgruppen for denne aktivitet er primært it-arkitekterne bag løsningen, udviklerne og kommunens databeskyttelsesrådgiver samt it-sikkerhedsrådgiveren.

*Afkryds nedenfor de handlinger, som er blevet gennemført*

|  |  |
| --- | --- |
| [ ]  | Er AI-løsningen designet med henblik på at overholde de krav, der er blevet identificeret under aktiviteten ”kravsætning”?  |
|[ ]  Er AI-løsningen designet under hensyntagen til de fem dataorienterede designprincipper: 1) Minimér og begræns, 2) Gem og skjul, 3) Adskil, 4) Aggregér og 5) Databeskyttelse gennem standardindstillinger? Brug her **Værktøj nr. 4**. |
| [ ]  | Er AI-løsningen designet under hensyntagen til de fire procesorienterede designprincipper: 1) Informér, 2) Kontrollér, 3) Håndhæv og 4) Demonstrér? For nærmere informationer om disse designprincipper, se **Værktøj nr. 4**.  |

Bemærkninger til ovenstående punkter:

|  |
| --- |
|  |

# Indsamling af data, træning og validering af modellen

Denne aktivitet har til formål at gennemføre træning og validering af selve modellen i AI-løsningen, herunder tilvejebringe et passende datagrundlag af høj kvalitet herfor. Træningen af modellen – og dermed indsamlingen af data til brug herfor – afhænger af modellens karakter, herunder om det er en dynamisk eller statisk model, samt af hvad den skal kunne opnå (formålet og målsætningerne).

Aktiviteten indebærer, at kommunen får et overblik over sit databehov, herunder om der er mulighed for at indsamle eller have adgang til sådanne data af en tilstrækkelig kvalitet. Det er retligt afgørende for projektet, at de datatyper, som bruges til at træne og udvikle modellen – og som skal bruges som input i modellen, når modellen skal anvendes – også er retligt tilgængelige, når modellen efterfølgende skal implementeres og anvendes.

Det er vigtigt at være opmærksom på, at databeskyttelsesforordningens og -lovens regler, herunder de grundlæggende principper, kravet om hjemmel, de registreredes rettigheder og sikkerhedsmæssige krav, også gælder for personoplysninger, der anvendes under træning og validering af modellen.

For så vidt angår retsgrundlaget for behandlingen af personoplysninger i forbindelse med træning af modellen i løsningen (*udvikling*), vil kommunerne efter omstændighederne kunne anvende databeskyttelsesforordningens artikel 6, stk. 1, litra e, om behandling af personoplysninger, der er nødvendig af hensyn til udførelse af en opgave i samfundets interesse eller som henhører under offentlig myndighedsudøvelse, som den dataansvarlige har fået pålagt. Tilsvarende gælder databeskyttelseslovens § 10, stk. 1, hvorefter følsomme personoplysninger og oplysninger om strafbare forhold må behandles, hvis dette alene sker med henblik på at udføre statistiske eller videnskabelige undersøgelser af væsentlig samfundsmæssig betydning, og hvis behandlingen er nødvendig af hensyn til udførelsen af undersøgelserne.

Ved *anvendelse* af løsningen på konkrete sager som led i kommunens offentlige myndighedsudøvelse vil kommunen ofte kunne behandle personoplysningerne med hjemmel i særlovgivningen på det pågældende sagsområde sammenholdt med databeskyttelsesforordningens artikel 6, stk. 1, litra e, og artikel 9, stk. 2, litra f, om behandling, der er nødvendig, for at retskrav kan fastlægges, gøres gældende eller forsvares, eller når domstole handler i deres egenskab af domstol.

Retsgrundlaget for kommunens behandling af personoplysninger vil derfor ofte ikke være samtykke fra de registrerede. Et samtykke kræver, at det er indgået frivilligt. Kommunen skal i relation til dette frivillighedskrav være opmærksom på, om der foreligger et ulige forhold mellem den dataansvarlige og den registrerede, da der i så fald ikke vil være tale om et gyldigt samtykke. Det kan f.eks. være tilfældet, hvis der er tale om en sag, hvor den registrerede ansøger om en offentlig ydelse hos kommunen. Den registrerede vil i dette tilfælde oftest ikke have andre alternativer end at give samtykke til behandlingen, hvis borgeren vil have ydelsen. Kommunen vil derfor ofte ikke kunne behandle personoplysninger på baggrund af et samtykke. Kommunen bør af denne grund nøje overveje anvendelsen af samtykke som behandlingsgrundlag. Hvis kommunen har brug for oplysningen, dvs. at kommunen som følge af indretningen af lovgivningen ikke kan indhente de relevante oplysninger på anden måde, kan kommunen dog anvende samtykke som behandlingsgrundlag.

En kommune må ikke uden videre bruge personoplysninger, som er indsamlet til ét formål, til at træne og anvende algoritmer, som skal bruges til et andet formål. Dette beror på, om reglerne om formålsbegrænsning er overholdt, jf. databeskyttelsesforordningens artikel 5, stk. 1, litra b, artikel 6, stk. 4, samt databeskyttelseslovens § 5 og § 10, stk. 2. Der kan endvidere være særlige tavshedspligtsregler efter særlovgivningen, som forhindrer, at personoplysninger anvendes i nye sammenhænge.

En kommune må som udgangspunkt ikke anvende andre kommuners træningsdata, der indeholder personoplysninger, til træning af kommunens egen AI-løsning. Dog kan der efter omstændighederne være mulighed herfor, f.eks. hvis videregivelsen sker udelukkende i statistisk øjemed eller hvis der indgås tværkommunale samarbejde med brug af fælles dataansvar.

Målgruppen for denne aktivitet er primært data scientists, der har et godt overblik over de tilgængelige data, deres kvalitet, komplethed og repræsentativitet. Databeskyttelsesrådgiveren skal også inddrages, ligesom det ofte vil være relevant at inddrage fageksperter, der har juridiske kompetencer inden for den særlovgivning og område, som løsningen vedrører.

*Afkryds nedenfor de handlinger, som er blevet gennemført*

|  |  |
| --- | --- |
| [ ]  | Er der indsamlet en tilstrækkelig mængde træningsdata af høj kvalitet til, at det er muligt at træne algoritmen på nødvendig vis, så modellen er tilstrækkeligt optimeret og træfsikker? Det skal sikres, at datagrundlaget er tilstrækkeligt nuanceret til, at algoritmen kan trænes i lignende situationer, som den skal anvendes på. |
|[ ]  Er det overvejet, om de registrerede skal informeres om databehandlingen efter oplysningspligten i databeskyttelsesforordningens artikel 13-14? |
|[ ]  Er det vurderet, om de datatyper, som bruges til at træne og udvikle modellen – og som skal bruges som input i modellen, når modellen skal anvendes – også er retligt tilgængelig, når modellen efterfølgende skal implementeres og anvendes? |
|[ ]  Er der udarbejdet dokumenterbare retningslinjer og procedurer for adskillelse af udviklings- og produktionsmiljø og dokumentation af, at adskillelsen er sket? |
| [ ]  | Er der etableret en procedure for begrænsning af personoplysninger i udviklingsmiljø, herunder for hvordan miljøet renses for personoplysninger, når disse ikke længere skal anvendes i udviklingsmiljøet? |
| [ ]  | Er der etableret en risikovurdering vedrørende behandlingssikkerhed, herunder en passende autorisations- og adgangskontrol, der sikrer, at kun personer med et legitimt formål har adgang til trænings- og testdata, hvis disse indeholder personoplysninger?  |
| [ ]  | Er der etableret en klar ansvarsfordeling af, hvem der har ansvaret for modellens performance, dvs. en klar og ansvarlig ejer af modellen, som vedligeholder modellen og har kompetence til at ændre og modificere koden. |
| [ ]  | Er behandling af personoplysninger i forbindelse med udvikling af AI-løsningen omfattet af kommunens fortegnelse over behandlingsaktiviteter? Hvis ikke, er der da udarbejdet en fortegnelse herfor? |

Bemærkninger til ovenstående punkter:

|  |
| --- |
|  |

# Konstruktion af AI-løsningen

Denne aktivitet har til formål at gøre udviklerne af AI-løsningen i stand til at kode løsningen på sikker vis gennem implementering af de krav, der er konstateret hidtil. Databeskyttelsesforordningens regler finder anvendelse under konstruktionen af AI-løsningen. Af denne grund er det vigtigt, at kommunen vælger en sikker og pålidelig tilgang til kodning og detektion af sårbarheder i algoritmen, så AI-løsningens algoritme udvikles under forsvarlige forhold.

Målgruppen for denne aktivitet er primært udviklerne af AI-løsningen, den it-sikkerhedsansvarlige, kommunens databeskyttelsesrådgiver og testere.

*Afkryds nedenfor de handlinger, som er blevet gennemført*

|  |
| --- |
|[ ]  Er der gennemført en risikoanalyse forud for godkendelsen af de valgte værktøjer og understøttende komponenter, herunder med fokus på privatlivsrisici og sikkerhedsmæssige sårbarheder? |
| [ ]  | Er der etableret en forretningsgang for regelmæssig kodeanalyse samt kodegennemgang, så det sikres, at retningslinjerne for sikker kodning overholdes samt at fejl eller uhensigtsmæssigheder i algoritmen opdages tidligst muligt for at begrænse skadevirkningerne heraf?  |

Bemærkninger til ovenstående punkter:

|  |
| --- |
|  |

# Test af AI-løsningen

Formålet med denne aktivitet er at teste AI-løsningen før release af løsningen og sikre, at de konstaterede krav og designmæssige principper faktisk er blevet implementeret og håndteret på passende vis i AI-løsningen. Derudover skal det under denne aktivitet også sikres, at AI-løsningens model er i stand til at nå frem til resultater med en tilfredsstillende grad af træfsikkerhed og på grundlag af korrekt afvejning af data. Det vil her ofte være relevant bl.a. at teste for, at AI-løsningen ikke indebærer ulovlig forskelsbehandling, f.eks. fordi modellen er trænet på baggrund af træningsdata, der indeholder en ulovlig vægtning af data.

Ved test i forbindelse med udvikling af AI-løsninger skal der som udgangspunkt anvendes egentlige testdata, dvs. oplysninger om fiktive personer, og ikke oplysninger om eksisterende personer. Der bør således ikke som testdata anvendes kopi af produktionsdata, medmindre der forinden er foretaget en effektiv anonymisering af disse. I de tilfælde, hvor det måtte være nødvendigt at benytte personoplysninger, vil databeskyttelsesreglerne finde fuldt ud anvendelse og de sikkerhedsforanstaltninger, som kræves herefter, skal således være på plads også i testen.

Målgruppen for denne fase er primært testere, kommunens databeskyttelsesrådgiver, sikkerhedsrådgiver, udviklere og projektlederen.

*Afkryds nedenfor de handlinger, som er blevet gennemført*

|  |  |
| --- | --- |
| [ ]  | Er det testet, at AI-løsningen imødekommer de krav, der blev fastlagt i løbet af aktiviteterne ”kravsætning” og ”design”?  |
| [ ]  | Er det vurderet, hvorvidt fiktive eller anonymiserede oplysninger kan anvendes som testdata? Og er denne vurdering blevet dokumenteret, f.eks. som led i konsekvensanalysen for AI-løsningen (**Værktøj nr. 2**)? |
| [ ]  | Hvis testdataene består af personoplysninger, er det så vurderet og dokumenteret, hvordan personoplysninger indgår i tests, samt hvorfor det er nødvendigt og sagligt at anvende personoplysninger i stedet for syntetiske eller anonymiserede oplysninger? |
| [ ]  | Hvis testdataene består af personoplysninger, hvilke tekniske sikkerhedsforanstaltninger, herunder adgangskontrol, er der i så fald gennemført for at sikre de personoplysninger, der findes i testmiljøer på forskellige stadier? |
| [ ]  | Hvis testdataene består af personoplysninger, findes der i så fald procedurer for begrænsning af personoplysninger i testmiljøer, herunder for hvordan testmiljøer renses for personoplysninger, når disse ikke længere skal være i systemet? |
|[ ]  Er der blevet gennemført og dokumenteret grundige test af modellen, herunder dens præcision, samt hvorvidt den afvejer data på ønsket og lovlig vis? |

Bemærkninger til ovenstående punkter:

|  |
| --- |
|  |

# Release af AI-løsningen

I løbet af denne aktivitet gøres det organisatoriske og tekniske miljø omkring AI-løsningen klar til release. Når AI-løsningen og det organisatoriske omkring løsningen vurderes klar til lancering, bliver AI-løsningen releaset til anvendelse i praksis. Formålet med denne aktivitet er at sikre, at release af AI-løsningen er godkendt på det relevante ledelsesniveau samt at der er lagt en plan for rettidig opdagelse og håndtering af hændelser ved release samt for løbende gennemgang og test af løsningen i drift.

Målgruppen for denne aktivitet er primært projektlederen, kommunens databeskyttelsesrådgiver og it-sikkerhedsrådgiver. Når planen for hændelseshåndtering udarbejdes, bør de personer, der kommer til at håndtere hændelserne i praksis, dog inddrages.

*Afkryds nedenfor de handlinger, som er blevet gennemført*

|  |  |
| --- | --- |
| [ ]  | Er der blevet udarbejdet en plan for håndtering af hændelser, herunder brud på persondatasikkerheden, der er relateret til AI-løsningen? Denne plan indeholder bl.a. beskrivelser af relevante kontaktpunkter, kommunikationskanaler til indrapportering af hændelser og teknisk support, svartider, procedurer for løbende risikohåndtering, anmeldelse til Datatilsynet og underretning af de registrerede m.v.  |
| [ ]  | Er AI-løsningen blevet endeligt godkendt af den relevante ledelse inden release – på baggrund af input fra projektlederen, databeskyttelsesrådgiveren og it-sikkerhedsrådgiveren?  |
| [ ]  | Er alle relevante dokumenter og data fra udviklingsprocessen blevet arkiveret, herunder bl.a. kravene til systemet og modellen (**Værktøj nr. 4**), kildekoden, binær kode, den gennemførte konsekvensanalyse (**Værktøj nr. 2**) og risikovurderinger m.v.? |
| [ ]  | Er der fastlagt en plan for rettidig detektion og håndtering af uhensigtsmæssigheder og fejl i AI-løsningen, herunder en fallback plan, der sikrer driftskontinuitet, hvis AI-løsningen fejler og må stoppes?  |
| [ ]  | Er der etableret en dokumenterbar proces for regelmæssig gennemgang og test af AI-løsningen, herunder ansvarsfordelingen herfor? |
| [ ]  | Er behandling af personoplysninger i forbindelse med anvendelse af AI-løsningen omfattet af kommunens fortegnelse over behandlingsaktiviteter? Hvis ikke, er der da udarbejdet en fortegnelse herfor? |
| [ ]  | Er de ansatte, der skal anvende AI-løsningen, blevet undervist i databeskyttelsesforordningens og -lovens krav, så de har en grundlæggende forståelse for de retlige krav, som AI-løsningen skal kunne overholde løbende i drift? |
| [ ]  | Er de ansatte, der skal anvende AI-løsningen, blevet undervist i de krav, der følger af relevant særlovgivning, standarder og interne regler, som AI-løsningen skal kunne overholde løbende i drift? |

Bemærkninger til ovenstående punkter:

|  |
| --- |
|  |

# Løbende kontrol i drift

Denne aktivitet består af den kontrol og overvågning af løsningen, der skal finde sted efter AI-løsningens idriftsættelse. Selvom AI-løsningen nu anvendes i praksis, skal der løbende følges op på løsningens indhold og håndtering af relevante hændelser gennem efterfølgende kontrolforanstaltninger. Der kan her være tale om både organisatoriske foranstaltninger, f.eks. interne procedurer for løbende overvågning af løsningen, såvel som tekniske foranstaltninger, f.eks. tekniske løsninger for at identificere sikkerhedsbrud.

Hvis løsningen skal udfases eller nedlukkes, vil det også være relevant at udarbejde en procedure herfor, herunder en fallback-plan.

Målgruppen for denne aktivitet er primært de ansatte, der er ansvarlige for at håndtere hændelser efter release, sikkerhedsrådgiveren, databeskyttelsesrådgiveren og ansatte der forvalter, drifter og vedligeholder AI-løsningen.

*Afkryds nedenfor de handlinger, som er blevet gennemført*

|  |  |
| --- | --- |
| [ ]  | Er planen for hændelseshåndtering implementeret og håndhævet? Kan vi dokumentere, hvordan vi har fulgt op på hændelser? |
| [ ]  | Er der fastlagt en klar og dokumenteret rolle- og ansvarsfordeling for den efterfølgende kontrol og test af AI-løsningen? Er det fastlagt, hvem der kontrollerer systemets performance? |
| [ ]  | Bliver AI-løsningen regelmæssigt testet og opdateret efter dokumenterede retningslinjer? Er det fastlagt, hvordan og hvor ofte systemet overvåges og opdateres? Gennemførte tests, resultater heraf samt foranstaltninger truffet i medfør heraf skal kunne dokumenteres. |
|[ ]  Er planen for detektion og håndtering af uhensigtsmæssigheder og fejl i AI-løsningen implementeret og håndhævet? |
|[ ]  Er relevant systemdokumentation, herunder dokumentation for kravene til løsningen (**Værktøj nr. 4**), risikovurderinger og konsekvensanalysen vedrørende databeskyttelse (**Værktøj nr. 3**), blevet opdateret ved ændringer? |
|[ ]  Bliver brud på persondatasikkerheden og rettighedsanmodninger fra registrerede effektivt håndteret indenfor de fastsatte tidsfrister? |
|[ ]  Bliver fortegnelserne vedrørende behandlingsaktiviteterne for løsningen vedligeholdt? |

Bemærkninger til ovenstående punkter:

|  |
| --- |
|  |