**Juridisk værktøjskasse for Ansvarlig AI**

**Værktøj nr. 2**

Skabelon til konsekvensanalyse vedrørende databeskyttelse for AI-løsninger

 

|  |
| --- |
| Konsekvensanalyse vedrørende databeskyttelse for *[AI-løsningens navn]* |

|  |  |
| --- | --- |
| Dataansvarlig: |  |
| Udfyldt af: |  |
| Ansvarlig kontaktperson: |  |
| Repræsentant for ledelsen: |  |
| Databeskyttelsesrådgiver: |  |
| System(er) der anvendes til projektet: |  |

**Versionsstyring**

|  |  |
| --- | --- |
| **Version, dato** | **Bemærkninger** |
| V.1, *[oprettelsesdato]* | Udarbejdelse af første version af konsekvensanalysen |
| V.2, *[opdateringsdato]* | *[Indsæt bemærkning om årsag til opdatering]* |
| V.3, *[opdateringsdato]* |  |

Indholdsfortegnelse

[Sammenfatning 4](#_Toc42075598)

[Indledning og baggrund 5](#_Toc42075599)

[Konsekvensanalysens formål 5](#_Toc42075600)

[Baggrunden for konsekvensanalysen 5](#_Toc42075601)

[1. Trin 1: Systematisk beskrivelse af behandlingen af personoplysninger i AI-løsningen 6](#_Toc42075602)

[1.1 AI-løsningens formål og karakter 6](#_Toc42075603)

[1.2 AI-løsningens behandling af personoplysninger og omfanget heraf 7](#_Toc42075604)

[1.3 Sammenhæng og kontekst for behandlingen af personoplysninger i AI-løsningen 8](#_Toc42075605)

[1.4 Modtagere af personoplysninger i AI-løsningen 9](#_Toc42075606)

[1.5 Opbevaringsperiode for personoplysninger i AI-løsningen 9](#_Toc42075607)

[2. Trin 2: Inddragelse af relevante interessenter 10](#_Toc42075608)

[2.1 Inddragelse af kommunens databeskyttelsesrådgiver (DPO) 10](#_Toc42075609)

[2.2 Indhentning af de registreredes eller deres repræsentanters synspunkter 10](#_Toc42075610)

[3. Trin 3: Projektets lovlighed, nødvendighed og proportionalitet 11](#_Toc42075611)

[3.1 Princippet om lovlighed, rimelighed og gennemsigtighed 11](#_Toc42075612)

[3.2 Princippet om formålsbegrænsning 12](#_Toc42075613)

[3.3 Princippet om dataminimering 12](#_Toc42075614)

[3.4 Princippet om rigtighed 13](#_Toc42075615)

[3.5 Princippet om opbevaringsbegrænsning 13](#_Toc42075616)

[3.6 Princippet om integritet og fortrolighed (sikkerhed og robusthed) 14](#_Toc42075617)

[3.7 Behandlingsgrundlag (hjemmel) 14](#_Toc42075618)

[3.8 De registreredes rettigheder 15](#_Toc42075619)

[3.9 Databehandlere 17](#_Toc42075620)

[3.10 Overførsel til tredjelande og/eller internationale organisationer 17](#_Toc42075621)

[4. Trin 4: Identifikation, evaluering og håndtering af risici 18](#_Toc42075622)

[4.1 Valg af evalueringskriterier for sandsynlighed og konsekvens 18](#_Toc42075623)

[4.2 Identifikation, evaluering og håndtering af behandlingsaktivitetens konkrete risici 20](#_Toc42075624)

[5. Trin 5: Konklusion og ledelsesgodkendelse 21](#_Toc42075625)

[5.1 AI-løsningens samlede restrisiko og høring af Datatilsynet 21](#_Toc42075626)

[5.2 Ledelsens godkendelse af konsekvensanalysen 21](#_Toc42075627)

[5.3 Bilag til konsekvensanalysen 22](#_Toc42075628)

[6. Trin 6: Ajourføring af konsekvensanalysen 23](#_Toc42075629)

[7. Bilag 24](#_Toc42075630)

# Sammenfatning

Konsekvensanalysen kan overordnet sammenfattes på følgende måde:

|  |
| --- |
| *[Her skal du skrive en kort sammenfatning af konsekvensanalysen, herunder navnlig følgende punkter:*   * *Hvorvidt ledelsen kan godkende konsekvensanalysen* * *Databeskyttelsesrådgiverens synspunkter* * *Hvorvidt Datatilsynet skal høres, inden AI-løsningen idriftsættes* * *De væsentligste risici for behandlingerne af personoplysninger i AI-løsningen* * *Hvilke væsentlige implementeringsskridt, som det anbefales, at der bliver foretaget.*   *Herudover skal det angives, hvordan der foretages kontrol af, om implementeringsskridtene er foretaget, samt hvordan processen fremadrettet vil være i forhold til løbende ajourføring af konsekvensanalysen.]* |

# Indledning og baggrund

## Konsekvensanalysens formål

|  |
| --- |
| *[Her skal du beskrive formålet med konsekvensanalysen. Nedenfor følger et forslag til tekst. Dette skal tilrettes, så det passer med de faktiske omstændigheder:*  *”Formålet med denne konsekvensanalyse vedrørende databeskyttelse er at beskrive den behandling af personoplysninger, som [den dataansvarlige kommune] vil foretage i forbindelse med [AI-løsningens navn].*  *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]](#footnote-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:

|  |
| --- |
| *[Her skal du kort beskrive, hvorfor du har vurderet, at din kommune som dataansvarlig er forpligtet til at foretage en konsekvensanalyse for AI-løsningen. Der skal som altovervejende udgangspunkt gennemføres konsekvensanalyser for nye AI-løsninger, der indebærer automatiseret beslutningstagen, herunder hvis denne er baseret på profilering, idet udviklingen og ibrugtagningen af AI-løsninger almindeligvis indebærer brug af nye teknologier og omfattende behandling af personoplysninger, hvilket sandsynligvis indebærer en høj risiko for registreredes rettigheder og frihedsrettigheder, jf. databeskyttelsesforordningens artikel 35, stk. 1.*  *Konsekvensanalysen kan også være ønskelig af andre grunde, f.eks. hvis du er i tvivl om, hvorvidt der er pligt til at lave analysen, eller hvis I ønsker at lave en konsekvensanalyse for at forbedre 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:

|  |
| --- |
| *[Her skal du beskrive formålene med AI-løsningen og dens behandling af personoplysninger. Denne beskrivelse skal navnlig forholde sig til følgende spørgsmål:*   * *Hvad er formålet/ene? Eksempler på formål kan være sagsbehandling, træffe afgørelser over for borgerne om ydelser, profilering med henblik på at forudsige borgernes behov for vejledning eller kontrolformål, f.eks. bekæmpelse af social svig.* * *Sker der viderebehandling af personoplysninger til andre formål end det formål, som de forskellige oplysninger blev indsamlet til?* * *Hvilke legitime interesser har kommunen i at behandle registreredes personoplysninger i forbindelse med behandlingsaktiviteten? Det kan f.eks. være, at behandlingen af personoplysninger har hjemmel i lov, eller skal ske som led i offentlig myndighedsudøvelse.* * *Hvad er det forventede udbytte af behandlingsaktiviteten for de registrerede?* * *Hvad er det forventede udbytte for kommunen og/eller samfundet som helhed?]* |

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

|  |
| --- |
| *[Her skal du helt grundlæggende beskrive, hvorfor og hvordan AI vil blive brugt til at behandle personoplysninger i løsningen. Denne beskrivelse skal navnlig forholde sig til følgende spørgsmål:*   * *Hvorfor er der valgt en AI-løsning til løsning af opgaven?* * *Hvilken form for AI-teknologi anvendes, f.eks. supervised machine learning, unsupervised learning etc.?* * *Anvendes en statisk model (en model, der ikke udvikler sig og ”lærer” af nye inputdata) eller en dynamisk model (en model, der løbende lærer af nye inputdata og derfor udvikler sig over tid)?* * *Anvendes der beslutningsstøtte eller fuldautomatiske afgørelser?* * *Beskriv i hvilke faser AI-processer og automatiserede beslutninger kan have virkning på de registrerede.* * *Identificer og registrer omfanget af enhver menneskelig indgriben i beslutningsprocessen og i hvilken fase heraf.* * *Beskriv hvordan et menneske kan omgøre en automatisk afgørelse eller et forslag til afgørelse.* * *Hvis I bruger beslutningsstøtte, hvordan sikres det da, at mennesket foretager en reel vurdering af systemets forslag til afgørelser og ikke blot lægger forslaget ukritisk til grund?* * *Anvendes der profilering?* * *Hvilke sikkerhedsforanstaltninger tænkes der anvendt, herunder i relation til databehandlere og underdatabehandlere?]* |

## AI-løsningens behandling af personoplysninger og omfanget heraf

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

|  |
| --- |
| *[Her skal du overordnet beskrive de kategorier af personoplysninger, som kommunen indsamler og behandler som led i AI-løsningen. Det gælder både ved udvikling og anvendelse af løsningen.*   * *Der kan f.eks. være tale om kontaktoplysninger, herunder navn, adresse og e-mail, oplysninger om fagforeningsmæssigt tilhørsforhold, ledighedshistorik, CV, oplysninger om lønforhold, helbredsoplysninger samt CPR-nummer.* * *Det skal fremgå, hvilke oplysninger der anvendes til træning og opbygning af modellen, validering og test af modellen samt anvendelse af modellen.*   *Du skal også give en overordnet praktisk beskrivelse af, hvordan personoplysningerne bliver håndteret fra indsamling til sletning, dvs. hvilke behandlinger personoplysningerne undergives i løbet af AI-løsningens livscyklus. Denne beskrivelse skal navnlig forholde sig til følgende spørgsmål:*   * *Hvordan indsamles dataene til AI-løsningen? Hvad er kilderne hertil?* * *Hvordan anvendes de indsamlede data efter indsamling?* * *Hvordan sker der træning, opbygning, test og anvendelse af AI-modellen?*   *Du skal også beskrive de aktiver, som personoplysningerne behandles af i løbet af behandlingsaktiviteten. Eksempler på disse enheder kan være:*   * *Hardware, dvs. det tekniske udstyr (maskiner og maskindele) som tilsammen udgør et computersystem* * S*oftware, dvs. ét eller flere programmer, der kan afvikles i et bestemt computersystem* * *Netværk, dvs. et antal computere og evt. andre elektroniske apparater som er forbundet med hinanden med henblik på deling eller udveksling af data* * *Fysiske personer* * *Papir og papirforsendelseskanaler*   *Hvis den praktiske gennemgang bedst illustreres af et dataflow (en grafisk oversigt over datastrømmene), kan du vedlægge et sådan dataflow som bilag til konsekvensanalysen.]* |

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

|  |
| --- |
| *[Her skal du beskrive, hvilket omfang behandlingen af personoplysninger i AI-løsningen har. Denne beskrivelse skal navnlig forholde sig til følgende spørgsmål:*   * *Hvilke kategorier af registrerede personer behandles der personoplysninger om (f.eks. børn, ledige borgere, pårørende etc.)?* * *Hvor stort antal af registrerede behandles der personoplysninger om?* * *Hvor mange personoplysninger behandles? Dette spørgsmål gælder både omfanget af behandlingen af personoplysninger samt de behandlede personoplysningers detaljeringsgrad, dvs. evnen til at identificere de registrerede.* * *Hvor ofte behandles personoplysningerne i AI-løsningen, herunder hvorvidt behandlingen af personoplysningerne er enkeltstående, midlertidig, regelmæssig og kontinuerlig m.v.?* * *Hvilke geografiske områder dækker AI-projektet? Dette spørgsmål angår projektets geografiske udstrækning, herunder om personoplysningerne behandles lokalt, regionalt, nationalt, internationalt eller globalt.]* |

## 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:

|  |
| --- |
| *[Her skal du beskrive den sammenhæng, som AI-projektet indgår i, herunder hvilke interne og eksterne faktorer der kan påvirke de registreredes forventninger eller projektets konsekvenser. Denne beskrivelse skal navnlig forholde sig til følgende spørgsmål:*   * *Hvad er forholdet mellem den dataansvarlige og de registrerede under behandlingsaktiviteten?* * *I hvilket omfang har de registrerede kontrol over deres personoplysninger under behandlingsaktiviteten?* * *I hvilket omfang er behandlingsaktivitetens behandling af personoplysninger forudsigelig for de registrerede?* * *I hvilket omfang omfatter behandlingsaktiviteten børn eller andre sårbare registrerede?* * *I hvilket omfang har den dataansvarlige tidligere erfaring med den behandling af personoplysninger, som finder sted under behandlingsaktiviteten?]* |

## Modtagere af personoplysninger i AI-løsningen

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

|  |
| --- |
| *[Her skal du angive hvilke kategorier af modtagere (f.eks. databehandlere, andre offentlige myndigheder, andre borgere eller virksomheder m.v.), som personoplysningerne vil blive delt med udenfor den dataansvarliges organisation. I denne forbindelse skal du for hver kategori af modtagere angive, hvad formålet med delingen er.]* |

## Opbevaringsperiode for personoplysninger i AI-løsningen

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

|  |
| --- |
| *[Her skal du beskrive, hvor længe personoplysninger vil blive behandlet, herunder opbevaret, i forbindelse med AI-løsningen – både under udvikling og i drift. Denne beskrivelse skal navnlig forholde sig til følgende spørgsmål:*   * *Hvordan opbevares dataene under behandlingen?* * *Hvor længe behandles personoplysninger, inden de bliver uigenkaldeligt slettet eller anonymiseret, og med hvilken begrundelse?* * *Er der lavet retningslinjer for sletning, herunder slettetidspunkt og opfølgning på sletning m.v.?* * *Understøtter AI-løsningen og dets systemer effektiv og uigenkaldelig sletning?]* |

# 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:

|  |
| --- |
| *[Her kan databeskyttelsesrådgiverens bemærkninger angives. Hvis databeskyttelsesrådgiveren har rådgivet vedrørende et aspekt af konsekvensanalysen, som ikke er blevet efterkommet, bør begrundelsen herfor angives her.]* |

## 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

|  |
| --- |
| *[Hvis Ja: Beskriv de registreredes eller deres repræsentanters synspunkter, samt hvordan de er inddraget i konsekvensanalysen. Vedlæg eventuelle høringssvar som bilag. Hvis de registreredes eller deres repræsentanters synspunkter afviger fra konsekvensanalysen, bør du anføre begrundelsen herfor her.*  *Hvis Nej: Beskriv hvorfor du har vurderet, at de registreredes eller deres repræsentanters synspunkter ikke skal inddrages. Det kan f.eks. være irrelevant, hvis indhentelsen er umulig, uforholdsmæssigt upraktisk eller vanskelig at gennemføre, hvis indhentelsen kan underminere behandlingsaktivitetens sikkerhed eller hvis indhentelsen bør undlades af hensyn til kommercielle eller samfundsmæssige interesser, f.eks. hvis indhentelse vil skade fortroligheden i forbindelse med virksomheders forretningshemmeligheder.]* |

# 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.

|  |
| --- |
| *[Beskriv hvordan personoplysningerne i AI-løsningen bliver behandlet i overensstemmelse med princippet om lovlighed, rimelighed og gennemsigtighed.*  *Kravet om lovlighed indebærer bl.a., at behandlingerne af personoplysninger skal overholde databeskyttelsesreglerne og øvrig lovgivning.*  *Kravet om rimelighed indebærer overordnet set, at behandlingerne af personoplysningerne skal være rimelig over for de involverede registrerede og ikke må indebære ulovlig forskelsbehandling. Ved din vurdering skal du bl.a. tage hensyn til følgende spørgsmål:*   * *Hvilke foranstaltninger er implementeret, herunder kontrol og tests, der understøtter, at der ikke i træningsdata, modellen eller beslutninger er urimelige skævheder, der fører til ulovlig forskelsbehandling?*   *Kravet om gennemsigtighed indebærer, at behandlingerne af personoplysninger skal være tilstrækkeligt gennemsigtig og forudsigelig for de registrerede, så de lettere kan udøve kontrol over behandlingen af deres personoplysninger. I denne forbindelse skal det både være gennemsigtigt for de registrerede, at deres personoplysninger bliver behandlet, samt i hvilket omfang og hvordan deres personoplysninger bliver behandlet. Ved din vurdering skal du bl.a. tage hensyn til følgende spørgsmål:*   * *Hvordan sikres det, at behandlingen af registreredes personoplysninger er tilstrækkeligt gennemsigtig for de registrerede?* * *Hvordan sikres det, at det er muligt for os at forklare, hvordan AI-modellen kommer frem til en afgørelse, forslag til afgørelse eller forudsigelse?* * *Er det muligt for et menneske at forklare og forudse, hvordan systemets output (typisk en afgørelse eller forudsigelse) vil ændres, hvis inputdataene ændres?* * *Er det muligt for et menneske at identificere de mest vigtige inputdata, der medfører et bestemt resultat?* * *Er det muligt for et menneske at identificere, hvornår et forslag til en afgørelse, en forudsigelse eller en afgørelse måske er forkert?* * *Er modellens algoritme dokumenteret, så det er muligt at spore, hvorfor en afgørelse fik et forkert udfald?* * *Er der gennemført foranstaltninger eller mekanismer, der sikrer, at registrerede bliver oplyst på gennemsigtig vis, hvis der sker væsentlige ændringer af behandlingen undervejs?]* |

## 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 for at være uforenelige med de oprindelige formål, jf. databeskyttelsesforordningens artikel 5, stk. 1, litra b.

|  |
| --- |
| *[Beskriv hvordan personoplysningerne i AI-løsningen bliver behandlet i overensstemmelse med princippet om formålsbegrænsning. I din vurdering skal du inddrage følgende spørgsmål:*   * *Har vi et overblik over alle formålene med behandlingen?* * *Er formålene (hvis flere) med behandlingen af personoplysningerne tilstrækkeligt definerede og specifikke og ikke vage (som f.eks. ”brug til administrative formål”)?* * *Er formålene saglige og inden for den kommunens forvaltningsområde?* * *Sker der viderebehandling af personoplysninger til nye formål, som de registrerede ikke er informeret om, eller som kan overraske de registrerede?* * *Medfører AI-løsningen samkøring af oplysninger fra registre/områder, der varetager forskellige formål, evt. i kontroløjemed?]* |

## 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.

|  |
| --- |
| *[Beskriv hvordan personoplysningerne i AI-løsningen bliver behandlet i overensstemmelse med princippet om dataminimering. I din vurdering skal du inddrage følgende spørgsmål:*   * *Forklar og begrund behovet for at indsamle og opbevare personoplysninger i AI-løsningens faser, dvs. bl.a. analyse, modelopbygning og træning samt anvendelse* * *Kan formålet opnås ved at begrænse – evt. helt undgå – behandlingen af personoplysninger?* * *Kan formålet opnås ved brug af anonymiserede, aggregerede eller pseudonymiserede oplysninger?* * *Kan formålet opnås ved at behandle færre eller mindre detaljerede personoplysninger?* * *Er der personoplysninger, der indsamles, fordi de er ”nice to have” fremfor ”need to have”?* * *Kan det undgås at behandle følsomme personoplysninger eller oplysninger om strafbare forhold?* * *Kan behandlingsaktivitetens formål opnås med en mindre indgribende behandling af personoplysninger?]* |

## 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.

|  |
| --- |
| *[Beskriv i det følgende hvordan I sikrer, at der behandles korrekte og nødvendigt ajourførte personoplysninger i AI-løsningen. I din vurdering skal du inddrage følgende spørgsmål:*   * *Hvordan sikres det, at personoplysninger kan berigtiges og slettes, herunder ved brug af tekniske funktioner, automatiske og manuelle procedurer?* * *Hvordan sikres det, at personoplysningerne bliver registreret korrekt?* * *Hvordan sikres det, at der anvendes passende statistiske og matematiske procedurer til modeludviklingen?* * *Hvordan sikrer I, at træningsdataene, som I træner modellen med, er korrekte og repræsentative for målgruppen/sagerne, som modellen skal anvendes på?* * *I hvilket omfang vil der løbende blive foretaget tests af, om personoplysningerne og resultaterne af behandlingen heraf fortsat er korrekte?* * *Er der overblik over, hvem personoplysninger deles med, så eventuelle modtagere af personoplysninger kan blive underrettet om berigtigelse af eventuelle urigtige oplysninger?]* |

## 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.

|  |
| --- |
| *[Beskriv hvordan behandlingen af personoplysningerne i AI-løsningen overholder princippet om opbevaringsbegrænsning. I din vurdering skal du inddrage følgende spørgsmål:*   * *Hvad er den nødvendige opbevaringsperiode for personoplysninger for hvert formål, som behandlingen forfølger? Slettes personoplysningerne så snart denne periode er udløbet?* * *Kan formålet med behandlingen opnås ved en kortere opbevaringsperiode?* * *Hvordan sikres det, at personoplysninger slettes eller anonymiseres effektivt alle de steder, hvor de opbevares, herunder på lokale og bærbare opbevaringsmedier samt i systemer?* * *Hvordan er proceduren for opfølgning på sletning?* * *Hvordan er proceduren for sletning i forbindelse med backups af databaser?]* |

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

Personoplysninger skal behandles på en måde, der sikrer tilstrækkelig sikkerhed for de pågældende perosnoplysninger, 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.

|  |
| --- |
| *[Beskriv hvordan kommunen sikrer, at personoplysningerne bliver behandlet på en tilstrækkeligt sikker måde i AI-løsningen. I din vurdering skal du inddrage følgende spørgsmål:*   * *Er der foretaget en risikovurdering vedrørende behandlingssikkerhed for behandlingen af personoplysninger i løsningen efter databeskyttelsesforordningens artikel 32?* * *Er ansvarlige for informationssikkerhed blevet inddraget i afklaringen af behandlingsaktivitetens risikobillede og fastlæggelsen af de tilstrækkelige tekniske og organisatoriske foranstaltninger?* * *Er der en fallback plan for videreførelse af behandlingen i AI-løsningen ved brug af menneskelig bistand, hvis AI-løsningen midlertidigt eller permanent skal stoppes?]* |

## Behandlingsgrundlag (hjemmel)

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

|  |
| --- |
| *[Beskriv hvad behandlingsgrundlagene er for behandling af hver kategori af personoplysninger og deres behandling i AI-løsningen. Du skal bl.a. tage hensyn til følgende spørgsmål:*   * *Er det sikret, at kommunen har gyldige behandlingshjemler for behandlingen af personoplysningerne gennem hele AI-løsningens livscyklus?* * *Hvad er hjemlen til træning/modeludvikling og til modelanvendelse for AI-løsningen?* * *Hvis behandlingen helt eller delvist sker ved brug af samtykke: Indsamles der et gyldigt samtykke i overensstemmelse med forordningens artikel 7, der er frivilligt? Kan I dokumentere samtykket efterfølgende og understøtte den registreredes ret til at trække samtykket tilbage?* * *Foretages der særlige behandlingsformer, der har skærpede hjemmelskrav, f.eks. profilering, samkøring i kontroløjemed, offentliggørelse eller brug af fuldautomatiske afgørelser? Og er disse særlige hjemmelskrav overholdt?]* |

## 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.

|  |
| --- |
| *[Beskriv, hvordan kommunen vil informere de registrerede om behandlingen af deres personoplysninger i AI-løsningen. Overvej følgende spørgsmål:*   * *Bliver de registrerede oplyst om, at deres personoplysninger indgår til træning af en AI-model?* * *Hvis I bruger profilering, bliver de registrerede så oplyst herom?* * *Hvis I bruger fuldautomatiske afgørelser, bliver de registrerede så informeret herom, samt får meningsfulde oplysninger om logikken heri samt betydningen og de forventede konsekvenser af en sådan behandling for den registrerede?* * *Er der undtagelser til oplysningspligten i projektet, f.eks. i medfør af databeskyttelsesforordningens artikel 13-14 eller databeskyttelseslovens § 22?]* |

### 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.

|  |
| --- |
| *[Beskriv, hvordan kommunen vil understøtte de registreredes indsigtsret i AI-løsningen. Overvej følgende spørgsmål:*   * *Er kommunen i stand til at give indsigt i både træningsdata (inputdata) og de personoplysninger, som AI-løsningen generer (output)?* * *Hvis I anvender profilering, hvordan sikres det i så fald, at der i tillæg til indsigt i inputdataene til at danne profilen, tillige kan gives indsigt i oplysninger om profilen og de segmenter, som den registrerede er blevet placeret i?* * *Hvis I bruger fuldautomatiske afgørelser, kan I da give de registrerede meningsfulde oplysninger om logikken heri samt betydningen og de forventede konsekvenser af en sådan behandling for den registrerede?* * *Er der undtagelser til indsigtsretten, f.eks. efter databeskyttelsesforordningens artikel 15 eller databeskyttelseslovens § 22?]* |

### 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.

|  |
| --- |
| *[Beskriv, hvordan kommunen vil sikre overholdelsen af berigtigelsesretten i AI-løsningen. Overvej følgende spørgsmål:*   * *Hvordan understøtter løsningen, at de registrerede kan få berigtiget de inputdata, der er blevet brugt til at træne modellen eller profilen, hvis der anvendes profilering?* * *Hvordan understøtter løsningen, at de registrerede kan få berigtiget outputdata, dvs. resultatet af en afgørelse eller selve profilen (”scoren”), som personen har fået tildelt, herunder hvis der anvendes profilering?* * *Gælder der undtagelser til berigtigelsesretten, f.eks. i medfør af databeskyttelseslovens § 22?]* |

### 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).

|  |
| --- |
| *[Her skal du beskrive, hvordan kommunen vil sikre overholde af disse rettigheder, samt om der gælder undtagelser til rettighederne. Sådanne undtagelser kan både fremgå af databeskyttelsesforordningen samt af databeskyttelseslovens § 22 eller af relevant særlovgivning.* |

### 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.

|  |
| --- |
| *[Her kan du beskrive, hvis kommunen har planlagt særlige foranstaltninger for sikre inddragelse af borgerne, herunder f.eks. særlige klagemuligheder m.v. Hvis der ikke foretages automatiske individuelle afgørelser i forbindelse med AI-projektet, skal du blot skrive ”N/A” i dette felt.]* |

## Databehandlere

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

Ja

Nej

|  |
| --- |
| *[Hvis Ja: Her skal du angive hvilke databehandlere, som kommunen anvender til behandlingen af personoplysninger i AI-løsningen, samt hvilken behandling databehandlerne foretager. Det er vigtigt, at kommunen har afklaret sit dataansvar i forhold til databehandlere og tredjeparter.*  *Det skal også beskrives, om der er foretaget risikovurderinger af databehandlernes behandling af personoplysninger samt indgået databehandleraftaler med databehandlerne, herunder om der anvendes underleverandører (underdatabehandlere).*  *Beskriv tillige, hvordan kommunen fører tilstrækkeligt tilsyn med databehandlere og evt. underdatabehandlere, herunder bl.a. for at sikre, at de overholder sikkerhedsregler og ikke handler udenfor databehandleraftalens instruks.]* |

## 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

|  |
| --- |
| *[Hvis Ja: Her skal du angive de pågældende lande og/eller internationale organisationer. Det skal også beskrives, hvad overførselsgrundlaget i så fald er for at overføre oplysningerne, f.eks. brug af EU-Kommissionens standardkontraktbestemmelser eller overførsel til et sikkert tredjeland m.v.]* |

# 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.:   * Man har erfaring med hændelsen inden for de sidste 12 måneder * 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.:   * Man har erfaring med hændelsen, men ikke inden for de sidste 12 måneder * Kendes fra andre offentlige myndigheder og private virksomheder i Danmark (omtales i pressen) |
| **2** | **Mindre sandsynligt**: Hændelsen forventes ikke at forekomme, herunder f.eks.:   * Ingen erfaring med hændelsen * 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.:   * Ingen erfaring med hændelsen * Kendes fra få andre offentlige myndigheder og private virksomheder, men ikke i Danmark |

I denne konsekvensanalyse anvendes følgende evalueringskriterier for konsekvens[[2]](#footnote-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. |

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*

Et billede, der indeholder bord

Automatisk genereret beskrivelse

## 

## Identifikation, evaluering og håndtering af behandlingsaktivitetens konkrete risici

|  |
| --- |
| *[På baggrund af evalueringskriterierne ovenfor skal du nu identificere og evaluere hver risiko, som behandlingsaktiviteten udgør i forhold til registreredes rettigheder og frihedsrettigheder. I denne forbindelse skal du også beskrive, hvordan kommunen har tænkt sig at håndtere risikoen ved hjælp af tekniske og organisatoriske foranstaltninger (afhjælpende foranstaltninger).*  *Hvis kommunen allerede har et koncept for identifikation, evaluering og håndtering af risici i konsekvensanalyser vedrørende databeskyttelse, kan du anvende dette. Hvis ikke, findes der i denne konsekvensanalysens* ***Bilag 1*** *en oversigt, der kan anvendes til dette formål.*  *I forbindelse med dette trin i konsekvensanalysen kan du til inspiration anvende* ***Værktøj nr. 3 – Risikokatalog****, der indeholder et overblik over en række typiske risici ved behandling af personoplysninger i AI-løsninger samt forslag til, hvordan risiciene kan håndteres.*    *Når du har identificeret de nødvendige afhjælpende foranstaltninger, kan du med fordel udfylde* ***Handlingsplanen*** *i* ***Bilag 2****. Handlingsplanen kan anvendes til at styre og understøtte gennemførelsen af alle de ønskede foranstaltninger indenfor nærmere fastsatte frister.]* |

# 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

|  |
| --- |
| *[Angiv en begrundelse for din vurdering. Hvis det ovenfor er angivet, at den samlede restrisiko for behandlingen er høj, har kommunen pligt til at foretage en forudgående høring af Datatilsynet, inden den påtænkte behandling af personoplysninger i AI-løsningen påbegyndes, jf. databeskyttelsesforordningens artikel 36. Det skal fremgå her, om der skal ske høring af Datatilsynet.]* |

## 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:

|  |
| --- |
| [Indsæt begrundelse] |

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:

|  |
| --- |
|  |

## Bilag til konsekvensanalysen

Følgende bilag vedlægges eventuelt til konsekvensanalysen:

Forudgående tærskelanalyse af behandlingsaktiviteten, dvs. vurdering af, hvorfor der skal

laves en konsekvensanalyse

Dataflow over behandlingsaktivitetens forløb

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

Risikovurdering vedrørende behandlingssikkerhed efter databeskyttelsesforordningens artikel 32

Databeskyttelsesrådgiverens bemærkninger

Indhentede synspunkter fra registrerede eller deres repræsentanter

Datatilsynets rådgivning i forbindelse med høringsprocessen

Handlingsplan for implementering af foranstaltninger til at håndtere de identificerede risici (**Bilag 2**)

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:

|  |
| --- |
| *[Indsæt beskrivelse af navn og titel på den ansvarlige person, inddragelse af DPO’en samt hvor ofte konsekvensanalysen skal revideres fast, f.eks. halv- eller helårligt, samt ved væsentlige ændringer/hændelser.]* |

# Bilag

**Bilag 1**: Skema til identifikation, evaluering og håndtering af risici i konsekvensanalysen

**Bilag 2**: Handlingsplan til implementering af foranstaltninger til håndtering af risici i konsekvensanalysen

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 [↑](#footnote-ref-1)
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 [↑](#footnote-ref-2)