Skabelon til Konsekvensanalyse vedrørende databeskyttelse (DPIA) i AI-projekter

|  |
| --- |
| Konsekvensanalyse (DPIA) vedrørende databeskyttelse for  |

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

|  |  |
| --- | --- |
| **Version** | **Kommentar** |
| 1.0, september 2025 | Udarbejdelse af første version af skabelon til konsekvensanalyse i overensstemmelse med Datatilsynets skabelon til DPIA ved AI af den 22. maj 2024 |

Indhold

[SAMMENFATNING 5](#_Toc205149295)

[INDLEDNING og BAGGRUND 6](#_Toc205149296)

[Konsekvensanalysens formål 6](#_Toc205149297)

[Konsekvensanalysens afgrænsning 6](#_Toc205149298)

[Baggrunden for konsekvensanalysen 7](#_Toc205149299)

[Forholdet til AI-forordningen 8](#_Toc205149300)

[1. TRIN 1: SYSTEMATISK BESKRIVELSE AF BEHANDLINGEN AF PERSONOPLYSNINGER I AI-LØSNINGEN 10](#_Toc205149301)

[1.1 AI-løsningens formål og karakter 10](#_Toc205149302)

[1.2 AI-løsningens behandling af personoplysninger og omfanget heraf 11](#_Toc205149303)

[1.3 Sammenhæng og kontekst for behandlingen af personoplysninger i AI-løsningen 13](#_Toc205149304)

[1.4 Modtagere af personoplysninger i AI-løsningen 14](#_Toc205149305)

[1.5 Opbevaringsperiode for personoplysninger i AI-løsningen 14](#_Toc205149306)

[2. TRIN 2: INDDRAGELSE AF RELEVANTE INTERESSENTER 15](#_Toc205149307)

[2.1 Inddragelse af databeskyttelsesrådgiver (DPO) 15](#_Toc205149308)

[2.2 Indhentning af de registreredes eller deres repræsentanters synspunkter 15](#_Toc205149309)

[3. TRIN 3: PROJEKTETS LOVLIGHED, NØDVENDIGHED OG PROPORTIONALITET 16](#_Toc205149310)

[3.1 Princippet om lovlighed, rimelighed og gennemsigtighed 16](#_Toc205149311)

[3.2 Princippet om formålsbegrænsning 18](#_Toc205149312)

[3.3 Princippet om dataminimering 18](#_Toc205149313)

[3.4 Princippet om rigtighed 19](#_Toc205149314)

[3.5 Princippet om opbevaringsbegrænsning 20](#_Toc205149315)

[3.6 Princippet om integritet og fortrolighed (sikkerhed og robusthed) 20](#_Toc205149316)

[3.7 Behandlingsgrundlag (hjemmel) 21](#_Toc205149317)

[3.8 De registreredes rettigheder 22](#_Toc205149318)

[3.8.1 Registreredes ret til underretning (oplysningspligten) 22](#_Toc205149319)

[3.8.2 Indsigtsretten 22](#_Toc205149320)

[3.8.3 Berigtigelsesretten 23](#_Toc205149321)

[3.8.4 Registreredes ret til sletning (retten til at blive glemt), ret til begrænsning, ret til dataportabilitet og indsigelsesret 24](#_Toc205149322)

[3.8.5 Registreredes ret til ikke at være genstand for automatiske individuelle afgørelser 24](#_Toc205149323)

[3.9 Databeskyttelse gennem design og gennem standardindstillinger 25](#_Toc205149324)

[3.10 Databehandlere 25](#_Toc205149325)

[3.11 Overførsel til tredjelande og/eller internationale organisationer 26](#_Toc205149326)

[4. TRIN 4: IDENTIFIKATION, EVALUERING OG HÅNDTERING AF RISICI 27](#_Toc205149327)

[4.1 Valg af evalueringskriterier for sandsynlighed og konsekvens 28](#_Toc205149328)

[4.2 Identifikation, evaluering og håndtering af behandlingsaktivitetens konkrete risici 30](#_Toc205149329)

[5. TRIN 5: KONKLUSION, LEDELSESGODKENDELSE og offentliggørelse 32](#_Toc205149330)

[5.1 Den samlede restrisiko ved behandlingen af personoplysninger i AI-løsningen og høring af Datatilsynet 32](#_Toc205149331)

[5.2 Ledelsens godkendelse af konsekvensanalysen 32](#_Toc205149332)

[5.3 Offentliggørelse af konsekvensanalysen 33](#_Toc205149333)

[5.4 Bilag til konsekvensanalysen 33](#_Toc205149334)

[6. TRIN 6: AJOURFØRING AF KONSEKVENSANALYSEN 34](#_Toc205149335)

[Bilag 1: Skema til identifikation, evaluering og håndtering af risici i konsekvensanalysen vedrørende databeskyttelse 35](#_Toc205149336)

[Bilag 2: Handlingsplan for implementering af foranstaltninger til at håndtere risici i konsekvensanalysen 36](#_Toc205149337)

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.*
* *De væsentligste risici for behandlingerne af personoplysninger i AI-løsningen.*
* *Hvilke væsentlige implementeringsskridt, som det anbefales, at der bliver foretaget.*
* *Hvorvidt Datatilsynet skal høres, inden løsningen baseret på kunstig intelligens (herefter ”AI-løsningen”) udvikles/idriftsættes.*

*Herudover skal det angives, hvorvidt der er udestående foranstaltninger, som mangler at blive implementeret, og hvordan disse implementeres. Det skal også beskrives, hvordan processen fremadrettet vil være i forhold til løbende ajourføring af konsekvensanalysen, herunder hvem der er ansvarlig herfor.]* |

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 [kommunen] vil foretage i forbindelse med brugen af [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 konsekvens-analyses 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.”]* |

Konsekvensanalysens afgrænsning

|  |
| --- |
| *[Her skal du beskrive, hvorvidt konsekvensanalysen omfatter behandlingen af personoplysninger i både udviklings- og driftsfasen af AI-løsningen. Behandling af personoplysninger til udvikling og drift af en AI-løsning udgør hvert sit separate formål efter databeskyttelsesreglerne. Hver fase skal således bl.a. have sit eget hjemmelsgrundlag, ligesom de grundlæggende principper, de registreredes rettigheder samt oplysningspligten skal overholdes i hver fase.* *Det fremgår af Datatilsynets praksis, at som led i vurderingen af, om en AI-løsning skal udvikles, bør kommunen dog foretage en samlet vurdering af hele livscyklussen for AI-løsningen for at sikre, at kommunen også har identificeret et eventuelt behandlingsgrundlag for at sætte løsningen i drift efterfølgende.**Denne skabelon til en konsekvensanalyse lægger derfor op til, at du vurderer behandlingen af personoplysninger til både udvikling og drift af løsningen. Der er dog ikke noget til hinder for, at konsekvensanalysen alene omfatter drifts- og gentræningsfasen – og dermed ikke udvikling – hvis kommunen vil anvende en standard AI-løsning, som allerede er udviklet.**Såfremt AI-løsningen skal idriftsættes på eksisterende teknisk infrastruktur, bør der henvises til eksisterende risikovurderinger mv., og det skal gøres klart, at nærværende analyse er afgrænset til behandling af personoplysninger ved brug af den pågældende AI-løsning.]* |

Baggrunden for konsekvensanalysen

Årsagen til udarbejdelsen af denne konsekvensanalyse er følgende:

|  |
| --- |
| *[Her skal du kort beskrive, hvorfor du har vurderet, at kommunen er forpligtet til at foretage en konsekvensanalyse for AI-løsningen. Behandling af personoplysninger som led i udvikling og/eller drift af AI-løsninger vil næsten altid udløse flere af de kriterier, der er udslagsgivende for, om der skal gennemføres en konsekvensanalyse. Det skyldes:** *at AI anses som såkaldt ”ny teknologi”, hvilket udgør et af kriterierne i Datatilsynets liste over aktiviteter, der altid er underlagt kravet om en konsekvensanalyse, og*
* *at udvikling og/eller drift af AI ofte indebærer*
* *(i) behandling af særlige kategorier af oplysninger,*
* *(ii) behandling af oplysninger om sårbare personer eller*
* *(iii) behandling af personoplysninger i stort omfang, hvilket er tre øvrige kriterier, der fremgår af Artikel 29-gruppens retningslinjer om konsekvensanalyse.[[2]](#footnote-2)*

*Der skal tilsvarende 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 I er i tvivl om, hvorvidt der er pligt til at lave analysen, eller hvis I ønsker at lave en konsekvensanalyse for at forbedre databeskyttelsen.]* |

Forholdet til AI-forordningen

|  |
| --- |
| *[Her skal du beskrive, om konsekvensanalysen vedrørende databeskyttelse udarbejdes i sammenhæng med en konsekvensanalyse vedrørende grundlæggende rettigheder for højrisiko-AI-systemer (på engelsk: ”fundamental rights impact assessment”, herefter ”FRIA”) efter AI-forordningen.[[3]](#footnote-3)**Det følger hertil af AI-forordningens artikel 27, stk. 4, at hvis nogle af de forpligtelser, som FRIA’en omfatter, allerede er opfyldt som følge af en konsekvensanalyse vedrørende databeskyttelse, jf. artikel 35 i databeskyttelsesforordningen, supplerer FRIA’en denne konsekvensanalyse.* *Der er udarbejdet en skabelon til en FRIA, hvortil der henvises.]* |

Udarbejdes der en konsekvensanalyse vedrørende grundlæggende rettigheder for højrisiko-AI-systemer (på engelsk: ”fundamental rights impact assessment”, herefter ”FRIA”) efter AI-forordningens artikel 27 for AI-systemet i sammenhæng med denne konsekvensanalyse vedrørende databeskyttelse?

☐ Ja

☐ Nej

Hvis nej, anfør da begrundelse herfor:

# 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 formålet/ene med AI-løsningen og dens behandling af personoplysninger. Beskriv overordnet, hvad AI-løsningen skal bruges til, hvilke(n) forretningsproces(ser) løsningen skal understøtte, hvad der ønskes opnået mv. Beskriv, hvilke forretningsproces(ser) og behandlingsaktiviteter, der berøres af brugen af AI-løsningen og hvordan.* *Beskrivelsen skal navnlig forholde sig til følgende spørgsmål:** *Hvad er formålet/ene? Eksempler på formål kan være udvikling af AI-løsningen eller driftsformål såsom sagsbehandling og at træffe afgørelser over for borgerne om ydelser, f.eks. 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 udgør en retlig forpligtelse 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?*
* *Beskriv typen af løsning, modelvalg og designvalg.*
* *Hvilken form for AI-teknologi anvendes, f.eks. supervised machine learning, unsupervised learning etc.?*
* *Hvilke variable (features) indgår i modellen, og hvad er disse variablers vægt?*
* *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 (”rubber stamping”)?*
* *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, test og drift af løsningen. Beskriv, hvilke – om nogen – kategorier af personoplysninger, der indgår i trænings-, validerings-, test-, input- og outputdata. Det skal fremgå, hvilke ikke-følsomme, følsomme og fortrolige personoplysninger der behandles.** *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.*
* *Det skal også fremgå, om der indgår personoplysninger i selve AI-modellen. Se hertil Det Europæiske Databeskyttelsesråds (EDPB) ”Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models” af den 17. december 2024, som kan findes på EDPB’s hjemmeside her.*

*Vær særligt opmærksom på, hvorvidt der ved anvendelse af AI-løsningen kan udledes (nye) følsomme personoplysninger ved sammenstilling af personoplysninger. Det er i mange tilfælde muligt ved hjælp af AI-løsninger at udlede særlige kategorier af oplysninger ved at sammenstille en række oplysninger om de registrerede og på det grundlag drage konklusioner om f.eks. personens fysiske eller mentale helbred, politiske overbevisning eller seksuelle orientering.**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*
* *Software, 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 datastrøm-mene), 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, ansatte, tidligere ansatte og pårørende etc.)?*
* *Hvor stort antal af registrerede behandles der personoplysninger om ved opstart og på lang sigt?*
* *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 kommunen og de registrerede under behandlingsaktiviteten (f.eks. borgere, medarbejdere mv.)?*
* *I hvilket omfang har de registrerede kontrol over deres personoplysninger under behandlingsaktiviteten?*
* *I hvilket omfang er behandlingsaktivitetens behandling af personoplysninger forudsigelig for de registrerede?*
* *Er der særlige udtalte bekymringer, f.eks. blandt de berørte personer eller i offentligheden, som bør indregnes?*
* *I hvilket omfang omfatter behandlingsaktiviteten børn, ældre, patienter, handicappede eller andre sårbare registrerede?*
* *I hvilket omfang har kommunen 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, borgere eller virksomheder m.v.), som personoplysningerne vil blive delt med udenfor kommunens organisation. I denne forbindelse skal du for hver kategori af modtagere angive, hvordan delingen foregår og 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, i forbindelse med test 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 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 om den planlagte behandlingsaktivitet. 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 samfundsmæssige interesser.]* |

# 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.* * *Beskriv vurderingen af, hvilket behandlingsgrundlag der muliggør behandling af personoplysninger til såvel udvikling som drift af AI-løsningen. Beskriv vurderingen separat for udvikling og for drift af løsningen. Hvis drift af AI-løsningen understøtter eller berører flere forretningsprocesser eller behandlingsaktiviteter, beskriv da behandlingsgrundlaget særskilt for de pågældende behandlingsaktiviteter.*
* *Beskriv, hvis relevant, vurderingen af, hvilken undtagelse til det generelle forbud mod behandling af* ***særlige kategorier af oplysninger*** *efter databeskyttelsesforordningens artikel 9, stk. 2, der muliggør behandling af sådanne kategorier til såvel udvikling som drift af AI-løsningen. Beskriv vurderingen separat for udvikling og for drift af løsningen.*
* *Beskriv, hvis relevant, vurderingen af, hvilket behandlingsgrundlag, der muliggør behandling af oplysninger om* ***strafbare forhold*** *til såvel udvikling som drift af AI-løsningen. Beskriv vurderingen separat for udvikling og for drift af løsningen.*
* *Beskriv, hvis relevant, vurderingen af, hvilket behandlingsgrundlag, der muliggør behandling af* ***oplysninger om personnummer*** *til såvel udvikling som drift af AI-løsningen. Beskriv vurderingen separat for udvikling og for drift af løsningen.*
* *Særligt for behandlingsaktiviteter i forbindelse med udvikling og test skal det beskrives, hvordan det sikres, at der i trænings- og testdata ikke indgår data, som er resultatet af brud på persondatasikkerheden eller i øvrigt er ulovligt tilvejebragt.*
* *Hvis der anvendes en AI-model købt af en leverandør, skal der endvidere foretages en vurdering af, hvorvidt AI-modellen indeholder personoplysninger, og i så fald skal der foretages en passende vurdering af, om oplysningerne er lovligt tilvejebragt af leverandøren. Se hertil ”Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models” af den 17. december 2024, som kan findes på EDPB’s hjemmeside her.*

*Kravet om rimelighed indebærer overordnet set, at behandlingerne af personoplysningerne skal være rimelig over for de involverede registrerede og ikke må indebære ulovlig forskelsbehandling.* * *Beskriv hvilke udfordringer eller problemstillinger den påtænkte brug af AI-løsningen skal adressere, og hvilke konkrete målsætninger brugen af løsningen har. Hvis der på dette tidlige stadie er klarhed over, hvilke problemstillinger AI-løsningen skal adressere og hvordan, er det lettere at vurdere, om løsningens output indebærer urimelige udfald for de registrerede.*
* *Særligt for behandlingsaktiviteter i forbindelse med udvikling og test skal det beskrives, hvordan det sikres, at træningsdata er retvisende, repræsentativt, og at eventuel tidligere bias håndteret. Beskriv endvidere, hvordan det igennem model- og designvalg sikres, at AI-løsningen ikke genererer urimeligt output eller resulterer i ulovlig forskelsbehandling.*
* *Særligt for behandlingsaktiviteter i forbindelse med drift skal det beskrives, hvordan det sikres, at AI-løsningen i drift ikke genererer urimeligt output, f.eks. ved løbende overvågning og test, og hvordan eventuel bias i output opdages og håndteres.*

*Kravet om gennemsigtighed indebærer, at behandlingerne af personoplysninger skal være tilstrækkeligt gennemsigtige, forklarlige og forudsigelige for de registrerede, så de registrerede 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.* * *Beskriv vurderingen af, i hvilket omfang valg af model og designvalg understøtter evnen til at fortolke og forklare AI-løsningens output.*
* *Særligt for behandlingsaktiviteter i forbindelse med udvikling og test skal det beskrives, hvordan det sikres gennem model- og designvalg samt implementering af foranstaltninger i øvrigt, at AI-løsningens output kan forklares.*
* *Særligt for behandlingsaktiviteter i forbindelse med drift skal det beskrives, hvordan det sikres, at output kan forklares, f.eks. hvis output danner grundlag for en beslutning over for den registrerede.*
 |

## 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 vurderingen af, i hvilket omfang formålet med behandling af personoplysninger ved udvikling og drift af AI-løsningen er sagligt og specifikt. Beskriv endvidere i hvilket omfang brug af de påtænkte datasæt til træning og test er foreneligt med det formål, som data oprindeligt er indsamlet til.]*
 |

## 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 i hvilket omfang behandling af persondata ved udvikling og drift af AI-løsningen er egnet, nødvendig og forholdsmæssig.* * *Beskriv afvejningen mellem det overordnede hensyn til de registrerede over for de hensyn, der taler for at udvikle og bruge AI-løsningen.*
* *Beskriv hvordan AI-løsningen udvikles, trænes og drives ved brug af færrest muligt oplysninger, og om muligt uden persondata.*
* *Beskriv hvilke privatlivsfremmende teknologier, der er blevet overvejet for at minimere mængden af persondata til udvikling, f.eks. fødereret læring eller syntetiske data*
* *Særligt for behandlingsaktiviteter i forbindelse med udvikling og test skal det beskrives, hvordan det sikres, at mængden af trænings- og testdata er begrænset til det nødvendige, og at der i det enkelte datasæt ikke indgår datapunkter, som ikke er nødvendige til træning og test.*
* *Særligt for behandlingsaktiviteter i forbindelse med drift skal det beskrives, hvordan det sikres, at input er begrænset til det nødvendige og relevante, og at der ikke indgår unødvendige data.]*
 |

## 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?*
* *Særligt for behandlingsaktiviteter i forbindelse med drift skal det beskrives, hvordan det sikres, at AI-løsningen fortsat genererer korrekte og retvisende output, f.eks. hvordan løbende modeldrift opdages og afhjælpes, hvordan statiske modeller overvåges og om nødvendigt gentrænes mv.*
* *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?*

*Særligt for behandlingsaktiviteter i forbindelse med udvikling og test skal det beskrives, hvordan det sikres, at trænings- og testdata er korrekte og retvisende.* |

## 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, herunder udvikling og drift af AI-løsningen, 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 personoplysninger, herunder beskyttelse mod uautoriseret eller ulovlig behandling og mod hændeligt tab, tilintetgørelse eller beskadigelse, under anvendelse af passende tekniske eller organisatoriske foranstaltninger, jf. databeskyttelsesforordningens artikel 5, stk. 1, litra f.

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

|  |
| --- |
| *[Beskriv hvordan kommunen sikrer, at personoplysningerne bliver behandlet på en tilstrækkeligt sikker måde igennem hele AI-løsningens livscyklus. 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? Denne vedlægges som bilag.*
* *Beskriv, hvordan brud på persondatasikkerheden håndteres, og hvordan de registrerede eventuelt underrettes om brud, som sandsynligvis vil indebære en høj risiko for de pågældende.]*
* *Er ansvarlige for informationssikkerhed blevet inddraget i afklaringen af behandlingsaktivitetens risikobillede og fastlæggelsen af de tilstrækkelige tekniske og organisatoriske foranstaltninger?*
* *Er der foretaget fornødne tests?*
* *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 samt særlovgivningen.

|  |
| --- |
| *[Beskriv hvad behandlingsgrundlagene er for behandling af hver kategori af personoplysninger og formålet med 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 automatiske, individuelle 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. Vær opmærksom på, at de registrerede som udgangspunkt skal underrettes om, at deres personoplysninger anvendes til både udvikling og drift, idet udvikling og drift udgør selvstændige formål. Overvej bl.a. 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 og konsekvenserne heraf, jf. præambelbetragtning 60?*
* *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 databeskyttelses-forordningens 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 samtlige personoplysninger, herunder i trænings-, validerings-, test-, input- og outputdata, herunder de eventuelle nye, selvstændige personoplysninger, som AI-løsningen genererer?*
* *Hvis I anvender profilering, hvordan sikres det i så fald, at der i tillæg til indsigt i in-putdataene 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, eller i drift?*
* *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?*
* *Hvordan kan underretning af eventuelle modtagere af ukorrekte oplysninger ske?]*
 |

### 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. Overvej bl.a. følgende spørgsmål:* * *Beskriv hvordan det sikres, at anmodninger om sletning håndteres korrekt, herunder om de registrerede kan få slettet eventuelle oplysninger i træningsdata eller i output, samt hvordan underretning af eventuelle modtagere af oplysninger, der skal slettes, kan ske.*
* *Beskriv, hvis det er relevant, hvordan det sikres, at anmodninger om dataportabilitet håndteres korrekt.*
* *Beskriv, hvis det er relevant, hvordan det sikres, at de registrerede har ret til at gøre indsigelse med hensyn til brug af vedkommendes data til udvikling af løsningen, eller mod at oplysningerne bruges som input.]*
 |
|  |

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

Det følger af databeskyttelsesforordningens 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. automatiske, individuelle afgørelser uden menneskelig indgriben. Denne rettighed finder dog ikke anvendelse, hvis afgørelsen (a) er nødvendig for indgåelsen eller opfyldelsen af en kontrakt mellem den registrerede og en dataansvarlig, (b) har hjemmel i dansk lov eller EU-retten, eller (c) er baseret på den registreredes udtrykkelige samtykke. I så fald kan de automatiske individuelle afgørelser lovligt finde sted.

|  |
| --- |
| *[Beskriv, hvis det er relevant, hvordan det sikres, at de registrerede har ret til menneskelig indgriben med hensyn til AI-løsningens output, kan fremkomme med sine synspunkter og bestride afgørelsen. Hvis der ikke foretages automatiske individuelle afgørelser i forbindelse med AI-projektet, skal du blot skrive ”N/A” i dette felt.]* |

## Databeskyttelse gennem design og gennem standardindstillinger

Det følger af databeskyttelsesforordningens artikel 25, stk. 1, om databeskyttelse gennem design, at den dataansvarlige – ud fra en risikobaseret tilgang – skal gennemføre passende tekniske og organisatoriske foranstaltninger, som er designet med henblik på både effektiv implementering af databeskyttelsesprincipper og med henblik på integrering af de fornødne garantier i behandlingen for at opfylde kravene i databeskyttelsesforordningen og beskytte de registreredes rettigheder.

Efter artikel 25, stk. 2, om databeskyttelse gennem standardindstillinger, skal den dataansvarlige gennemføre passende tekniske og organisatoriske foranstaltninger med henblik på gennem standardindstillinger at sikre, at kun personoplysninger, der er nødvendige til hvert specifikt formål med behandlingen, behandles. Denne forpligtelse gælder den mængde personoplysninger, der indsamles, og omfanget af deres behandling samt deres opbevaringsperiode og tilgængelighed. Sådanne foranstaltninger skal navnlig gennem standardindstillinger sikre, at personoplysninger ikke uden den pågældende fysiske persons indgriben stilles til rådighed for et ubegrænset antal fysiske personer.

|  |
| --- |
| *[Beskriv, hvordan kommunen vil sikre overholdelsen af pligten til databeskyttelse gennem design og gennem standardindstillinger i forhold til behandlingen af personoplysninger i AI-løsningen i hele løsningens livscyklus. Vedlæg eventuelt et selvstændigt bilag med en mere detaljeret vurdering heraf, herunder med fastsættelse af funktionelle og non-funktionelle krav til løsningsdesign m.v.]* |

## Databehandlere

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

☐ Ja

☐ Nej

|  |
| --- |
| *[Hvis Ja: Beskriv, hvilke databehandlere der benyttes som led i udvikling og drift af AI-løsningen, hvilken behandling der foretages af disse, samt hvilke fornødne garantier databehandlerne har givet for, at behandlingen sker i overensstemmelse med databeskyttelsesreglerne. Dette kan med fordel beskrives i bilag.* *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).**Vær også opmærksom på at vurdere, hvorvidt kommunen forbeholder sig ret til at anvende de overladte personoplysninger til databehandlerens egne formål, herunder f.eks. markedsføring, træning af AI-løsning eller anden form for produktudvikling m.v. I så fald vil der være tale om en videregivelse, som skal have hjemmel, ligesom kravet om formålsbegrænsning skal overholdes, jf. artikel 5, stk. 1, litra b.**Beskriv tillige, hvordan kommunen fører tilstrækkeligt tilsyn med databehandlere og eventuelle 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 den dataansvarlige 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., samt i hvilket omfang overførselsgrundlaget er effektivt. Dette kan med fordel beskrives i bilag.* *Hvis der skal overføres personoplysninger til et usikkert tredjeland, skal der foretages en vurdering af, hvilke supplerende foranstaltninger der skal implementeres for at sikre en beskyttelse af personoplysningerne, der sammen med overførselsgrundlaget sikrer et beskyttelsesniveau, som i det væsentlige svarer til niveauet i EU/EØS. Henvis eventuelt til en selvstændig såkaldt Transfer Impact Assessment med en vurdering af overførslernes lovlighed i et selvstændigt bilag til denne konsekvensanalyse.]* |

# 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. kompromittering af personoplysninger som følge af et hackerangreb. En risiko kan tillige vedrøre en utilsigtet manglende overholdelse af øvrige af forordningens regler, f.eks. risikoen for dataophobning i strid med dataminimeringsprincippet, overdreven indsamling af personoplysninger, der ikke er proportional med formålet, uønskede ændringer og forsvundne personoplysninger, ulovlig viderebehandling af personoplysninger, automatiseringspartiskhed 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[[4]](#footnote-4):

*Tabel 1. Evalueringskriterier for sandsynlighed*



I denne konsekvensanalyse anvendes følgende evalueringskriterier for konsekvens[[5]](#footnote-5):

*Tabel 2. Evalueringskriterier for konsekvens*



Når evalueringskriterierne for sandsynlighed og konsekvens er fastlagt, kan hver enkelt identificeret risiko vurderes og kortlægges i en såkaldt risikomatrix. I denne konsekvensanalyse anvendes følgende risikomatrix[[6]](#footnote-6):

Figur 1. Risikomatrix



## 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. Det er vigtigt, at du beskriver hver enkelt risiko samt de potentielle skadevirkninger i forhold til de 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 konsekvensanalyses* ***Bilag 1*** *et skema, der kan anvendes til dette formål.**I forbindelse med dette trin i konsekvensanalysen kan du til inspiration anvende* ***Risikokataloget****, der er udarbejdet til brug for gennemførelse af konsekvensanalysen, og som 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, LEDELSESGODKENDELSE og offentliggørelse

## Den samlede restrisiko ved behandlingen af personoplysninger i AI-løsningen og høring af Datatilsynet

På baggrund af de samlede risikoscorer efter afhjælpende foranstaltninger, 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:

|  |
| --- |
|  |

## Offentliggørelse af konsekvensanalysen

|  |
| --- |
| *[Offentliggørelse af konsekvensanalysen vedrørende databeskyttelse er ikke et retligt krav efter databeskyttelsesforordningen. Det er kommunens beslutning, om dette skal gøres. Men kommunen bør som minimum overveje at offentliggøre dele af konsekvensanalysen eller et resumé af konsekvensanalysen vedrørende databeskyttelse.]* |

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

☐ Mitigerende foranstaltninger og handlingsplan for implementering af foranstaltninger til at håndtere de identificerede risici (**Bilag 2**)

☐ Andre (indsættes i kommentarboks nedenfor):

|  |
| --- |
|  |

# TRIN 6: AJOURFØRING AF KONSEKVENSANALYSEN

Den dataansvarlige 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 1: Skema til identifikation, evaluering og håndtering af risici i konsekvensanalysen vedrørende databeskyttelse

|  |  |  |
| --- | --- | --- |
| **Identifikation** | **Evaluering** | **Håndtering** |
| Risikonr. | Navn på risiko | Beskrivelse af risikoens karakter og kilde | Risikoens skønnede konsekvenser *før* afhjælpende foranstaltninger | Risikoens skønnede sandsynlighed *før* afhjælpende foranstaltninger | Samlet risikoscore *før* afhjælpende foranstaltninger | Afhjælpende foranstaltninger | De afhjælpende foranstaltningers effekt på risikoen  | Risikoens skønnede konsekvenser *efter* afhjælpende foranstaltninger | Risikoens skønnede sandsynlighed *efter* afhjælpende foranstaltninger | Samlet risikoscore *efter* afhjælpende foranstaltninger |
| Indsæt nummeret på den identificerede risiko. | Indsæt titlen på den identificerede risiko. | Indsæt en kortfattet beskrivelse af risikoen, herunder hvordan risikoen udgør en trussel mod registreredes rettig­heder og frihedsrettig­heder | Beskriv de skønnede konsekvenser (skadevirkninger) for de registrerede. Angiv 1-4 baseret på evalueringskriterierne, der kan findes under afsnit 4.1. i konsekvensanalysen. | Angiv 1-4 baseret på evalueringskriterierne, der kan findes under afsnit 4.1. i konsekvensanalysen. | Indsæt det risikoniveau, der passer til behandlingsaktivitetens konsekvens- og sandsynlighedsniveau *inden* afhjælpende foranstaltninger. Scoren kan aflæses af Figur 1 under afsnit 4.1. i konsekvensanalysen. | Indsæt en beskrivelse af de foranstaltninger, den dataansvarlige vil gennemføre for at afhjælpe risikoens konsekvenser og sandsynlighed. | Angiv hvorvidt de afhjælpende medfører eliminering, reducering eller accept af risiko. | Angiv 1-4 baseret på evalueringskriterierne, der kan findes under afsnit 4.1. i konsekvensanalysen. | Angiv 1-4 baseret på evalueringskriterierne, der kan findes under afsnit 4.1. i konsekvensanalysen. | Indsæt det risikoniveau, der passer til behandlingsaktivitetens konsekvens- og sandsynlighedsniveau *efter* afhjælpende foranstaltninger. Scoren kan aflæses af Figur 1 under afsnit 4.1. i konsekvensanalysen. |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |

Bilag 2: Handlingsplan for implementering af foranstaltninger til at håndtere risici i konsekvensanalysen

I løbet af konsekvensanalysens Trin 4 er der identificeret en række foranstaltninger, der skal implementeres for at håndtere de databeskyttelsesmæssige risici i AI-løsningen. Nedenstående handlingsplan har til formål at understøtte, at foranstaltningerne implementeres rettidigt, dvs. inden behandlingen af personoplysninger i AI-løsningen påbegyndes.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Risikonummer** | **Afhjælpende foranstaltninger, der skal gennemføres** | **Frist for gennemførelse** | **Status på gennemførelse** | **Ansvarlig person** |
| Angiv nummeret på den risiko, som den afhjælpende foranstaltning knytter sig til. | Beskriv den relevante afhjælpende foranstaltning. | Angiv den valgte frist for gennemførelse. | Angiv status på gennemførelsen af den afhjælpende foranstaltning, f.eks. ”ikke påbegyndt”, ”i proces” eller ”færdig. | Angiv det fulde navn og rolle på den person, der er ansvarlig for at gennemføre den nævnte afhjælpende foranstaltning inden den valgte frist. |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

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. Datatilsynets vejledning om Offentlige myndigheders brug af kunstig intelligens – Inden I går i gang, oktober 2023, s. 37. [↑](#footnote-ref-2)
3. Europa-Parlamentets og Rådets forordning (EU) 2024/1689 af 13. juni 2024 om harmoniserede regler for kunstig intelligens og om ændring af forordning (EF) nr. 300/2008, (EU) nr. 167/2013, (EU) nr. 168/2013, (EU) 2018/858, (EU) 2018/1139 og (EU) 2019/2144 samt direktiv 2014/90/EU, (EU) 2016/797 og (EU) 2020/1828 (forordningen om kunstig intelligens). [↑](#footnote-ref-3)
4. Datatilsynet, skabelon til konsekvensanalyse ved AI, offentliggjort den 22. maj 2024. [↑](#footnote-ref-4)
5. Datatilsynet, skabelon til konsekvensanalyse ved AI, offentliggjort den 22. maj 2024. [↑](#footnote-ref-5)
6. Datatilsynet, skabelon til konsekvensanalyse ved AI, offentliggjort den 22. maj 2024 [↑](#footnote-ref-6)