Konsekvensanalyse for [Projekt/Behandlingsaktivitet]

Version […]

|  |  |
| --- | --- |
| Center: |  |
| Udfyldt af:  |  |
| Kontaktperson:  |  |
| Repræsentant for ledelsen:  |  |
| Databeskyttelsesrådgiver: |  |

Indhold

[Sammenfatning 4](#_Toc130986725)

[1. Baggrund og formål 5](#_Toc130986726)

[Baggrund 5](#_Toc130986727)

[Formålet med konsekvensanalysen 5](#_Toc130986728)

[Dataansvar 5](#_Toc130986729)

[2. Relevante parter 7](#_Toc130986730)

[Inddragelse af de registreredes synspunkter 7](#_Toc130986731)

[Inddragelse af kommunens Databeskyttelsesrådgiver 7](#_Toc130986732)

[3. Behandling af personoplysninger 8](#_Toc130986733)

[Formålet med behandlingen 8](#_Toc130986734)

[Behandlingens karakter og sammenhæng 8](#_Toc130986735)

[Kategorier af registrerede/ personoplysninger 8](#_Toc130986736)

[Behandlingens omfang 9](#_Toc130986737)

[4. Lovlighed, nødvendighed og proportionalitet 10](#_Toc130986738)

[Hjemmel til behandling af personoplysningerne 10](#_Toc130986739)

[Princippet om rimelighed og gennemsigtighed 10](#_Toc130986740)

[Princippet om formålsbegrænsning 10](#_Toc130986741)

[Princippet om dataminimering 11](#_Toc130986742)

[Princippet om rigtighed 12](#_Toc130986743)

[Princip om opbevaringsbegrænsning 12](#_Toc130986744)

[Princippet om fortrolighed og integritet 13](#_Toc130986745)

[Privacy by design 13](#_Toc130986746)

[Oplysningspligten 15](#_Toc130986747)

[Øvrige rettigheder 15](#_Toc130986748)

[5. Databehandlere, videregivelse og tredjelandsoverførsler 17](#_Toc130986749)

[Forholdet til databehandlere 17](#_Toc130986750)

[Videregivelse af personoplysninger 17](#_Toc130986751)

[Overførsel af personoplysninger til modtagere i tredjelande og internationale organisationer 17](#_Toc130986752)

[6. Risici samt foranstaltninger 19](#_Toc130986753)

[Valg af evalueringskriterier for konsekvens og sandsynlighed 19](#_Toc130986754)

[Identifikation, evaluering og håndtering af behandlingsaktivitetens konkrete risici 20](#_Toc130986755)

[7. Konklusion og ledelsesgodkendelse 21](#_Toc130986756)

[[Projektets/behandlingens] samlede restrisiko og høring af Datatilsynet 21](#_Toc130986757)

[Ledelsens godkendelse af konsekvensanalysen 21](#_Toc130986758)

[Bilag til konsekvensanalysen 22](#_Toc130986759)

[Ajourføring af konsekvensanalysen 22](#_Toc130986760)

# Sammenfatning

*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 projektet/behandlingsaktiviteten idriftsættes*
* *De væsentligste risici for behandlingerne af personoplysninger i projektet/behandlingsaktiviteten*
* *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.*

# 1. Baggrund og formål

## Baggrund

*Her skal du beskrive baggrunden for behandlingen, samt hvorfor kommunen er forpligtet til at foretage en konsekvensanalyse vedrørende databeskyttelse efter databeskyttelsesforordningens artikel 35 for projektet/behandlingsaktiviteten, eller om en sådan analyse er ønskelig af andre grunde.*

## Formålet med konsekvensanalysen

*Her skal du beskrive formålet med konsekvensanalysen.*

Forslag til tekst (skal rettes til):
Formålet med denne konsekvensanalyse vedrørende databeskyttelse er, at beskrive den behandling af personoplysninger, som Fredensborg Kommune foretager i forbindelse med [projektet/behandlingsaktiviteten].

Hvis relevant: Konsekvensanalysen omfatter ikke [indsæt beskrivelse, gerne evt. afgrænsning i forhold til andre projekter/behandlingsaktiviteter].

Hvis [projekt/ behandlingsaktiviteter] senere udvides til at omfatte […], vil denne konsekvensanalyse også blive opdateret, så den tillige omfatter behandlingen af personoplysninger forbundet hermed.”]

Konsekvensanalysen indeholder en vurdering af behandlingens lovlighed, dvs. om behandlingen overholder reglerne i databeskyttelsesforordningen og databeskyttelsesloven.

Konsekvensanalysen har til formål at afdække risici forbundet med den Kommunens behandling af personoplysninger som led i [projektet/behandlingen] samt at bidrage til at håndtere de risici for fysiske personers rettigheder og frihedsrettigheder, som behandlingen af personoplysninger medfører. Det sker ved at vurdere risici og fastlægge solide og effektive foranstaltninger til at afhjælpe dem.

Hvis konsekvensanalysen viser, at behandlingen af personoplysninger i forbindelse med [projektet/behandlingen] vil føre til en høj risiko for de registrerede i mangel af foranstaltninger truffet af Kommunen for at begrænse risikoen (residualrisikoen), skal Datatilsynet høres om behandlingen, inden behandlingen foretages, jf. databeskyttelsesforordningens artikel 36, stk. 1.

Konsekvensanalysen er en forudsætning for overholdelse af databeskyttelsesforordningens grundlæggende princip om ansvarlighed (dokumentation for overholdelse af forordningens regler), jf.
forordningens artikel 5, stk. 2, og artikel 24.

Hvis det er relevant, f.eks. ved IT-system eller app: Konsekvensanalysen har en naturlig sammenhæng til reglerne om databeskyttelse gennem design og gennem standardindstillinger, hvilket kan give værdifuldt input til håndtering af databeskyttelse i løsningsdesignet samt supplerende foranstaltninger.

## Dataansvar

*Du kan udelade dette afsnit, hvis der ikke er tvivl om dataansvaret, herunder fordi der ikke er flere aktører. Afsnittet skal tilpasses afhængigt af behandlingen og aktører.*

Forslag til tekst (skal rettes til):
Fredensborg Kommune har som udgangspunkt ansvaret for, at behandlingen af personoplysninger lever op til reglerne i databeskyttelsesforordningen. Der er flere forskellige aktører involveret i den behandling af personoplysninger, der sker i forbindelse med [projektet/behandlingen]. Det er derfor centralt at fastlægge, hvilke aktører der er ansvarlige for de enkelte dele af behandlingen af personoplysninger. Fredensborg Kommune er ansvarlig for den behandling af personoplysninger, der foretages hos kommunen selv. Når kommunen udveksler oplysninger med [navn på andre dataansvarlige] i forbindelse med [projektet/behandlingen], behandler parterne personoplysninger som selvstændige dataansvarlige. I visse tilfælde, herunder i forbindelse med […], behandler [virksomheds/myndigheds navn] dog personoplysninger som databehandler på vegne af Fredensborg Kommune.

# 2. Relevante parter

## Inddragelse af de registreredes synspunkter

*Hvis det er relevant, skal kommunen indhente de berørte borgeres eller deres repræsentanters synspunkter vedrørende den planlagte behandling. Om det er relevant, afhænger af en konkret vurdering af risiciene for borgerne. Hvis det vurderes relevant at inddrage borgerne, skal borgerne eller deres repræsentanters synspunkter beskrives og vedlægges.*

*Hvis kommunens endelige afgørelse afviger fra borgernes synspunkter, skal den kommunens begrundelse for at gå videre eller ikke dokumenteres i konsekvensanalysen. Hvis det ikke vurderes relevant at inddrage borgerne, skal det begrundes, hvorfor det ikke er relevant at inddrage borgerne eller deres repræsentanters synspunkter, f.eks. fordi en sådan inddragelse er umulig eller upraktisk, uforholdsmæssig, vil kunne underminere sikkerhed eller bør undlades af hensyn til kommercielle eller samfundsmæssige interesser, herunder grundet hastende karakter og efterfølgende offentlig oplysning samt frivillighed.*

*Hvis det vurderes, at det ikke er relevant at inddrage de registrerede, kan teksten indledes:*Fredensborg Kommune har vurderet, at det ikke er relevant at indhente de registreredes eller deres repræsentanters synspunkter vedrørende behandlingen af personoplysninger i forbindelse med [projektet/behandlingen], jf. databeskyttelsesforordningens artikel 35, stk. 9. Kommunen har lagt vægt på, at […].

## Inddragelse af kommunens Databeskyttelsesrådgiver

*Databeskyttelsesrådgiveren skal inddrages fra start og løbende i processen med udarbejdelse af en konsekvensanalyse, og DPO’ens synspunkter skal fremgå af konsekvensanalysen. I tilfælde af uenighed mellem organisationen og databeskyttelsesrådgiveren skal det fremgå af selve konsekvensanalysen, hvorfor databeskyttelsesrådgiverens indstilling ikke er blevet fulgt.*

Forslag til tekst (skal rettes til):
Databeskyttelsesrådgiveren for Fredensborg Kommune har været inddraget i processen med udarbejdelsen af denne konsekvensanalyse og er fremkommet med en række kommentarer hertil, som kommunen har forholdt sig til og inddraget i vurderingen.

[indsæt kommentarer]

# 3. Behandling af personoplysninger

## Formålet med behandlingen

*Her skal du beskrive formålet med behandlingen.*

*- Hvad er samtlige forskellige formål med behandlingen (f.eks. sagsbehandling, træffe (fuldautomatiske) afgørelser, profilering, kontrolformål, personaleadministration, statistik m.v.)?
- Hvad er det forventede udbytte for borgerne?
- Hvad er det forventede udbytte for kommunen eller samfundet som helhed?
- Sker der viderebehandling af personoplysninger til andre formål end det formål, som oplysningerne blev indsamlet til?*

## Behandlingens karakter og sammenhæng

*Her skal du beskrive konteksten for behandlingen, herunder interne og eksterne faktorer som kan påvirke borgernes forventninger eller konsekvenserne af behandlingen, herunder f.eks.:
- Hvad er forholdet til borgerne?
- Hvad er forholdet til eventuelle andre dataansvarlige?
- I hvilket omfang har borgerne kontrol over deres personoplysninger?
- I hvilket omfang kan borgerne anses for at kunne forvente behandlingen?
- Har borgerne særlige forventninger om fortrolighed og privatliv?
- I hvilket omfang omfatter behandlingen børn eller andre sårbare persongrupper, f.eks. patienter, handikappede m.v.?
- Hvor modtages oplysningerne fra?
- Hvem udveksles der oplysninger med?*

## Kategorier af registrerede/ personoplysninger

Skema rettes til ift. kategorier af registrerede (borgere, børn, medarbejdere, patienter mv.), og udfyldes:

|  |  |  |  |
| --- | --- | --- | --- |
| Typer af personoplysninger | Borgere | Børn, umyndiggjorte og andre sårbare  | Medarbejdere |
| Almindelige personoplysninger [Angiv hvilke almindelige oplysninger. Eksempelvis navn, telefonnummer, e-mail, adresse mm.] |  |  |  |
| Race eller etnisk oprindelse | [ ]  | [ ]  | [ ]  |
| Politisk overbevisning  | [ ]  | [ ]  | [ ]  |
| Religiøs overbevisning  | [ ]  | [ ]  | [ ]  |
| Filosofisk overbevisning  | [ ]  | [ ]  | [ ]  |
| Fagforeningsmæssigt tilhørsforhold  | [ ]  | [ ]  | [ ]  |
| Genetiske data | [ ]  | [ ]  | [ ]  |
| Biometriske data | [ ]  | [ ]  | [ ]  |
| Helbredsoplysninger, herunder misbrug af medicin, narkotika, alkohol m.v.  | [ ]  | [ ]  | [ ]  |
| En fysisk persons seksuelle forhold eller seksuelle orientering | [ ]  | [ ]  | [ ]  |
| Straffedomme | [ ]  | [ ]  | [ ]  |
| Lovovertrædelse | [ ]  | [ ]  | [ ]  |
| CPR-nr. | [ ]  | [ ]  | [ ]  |
| Andre fortrolige oplysninger [Angiv hvilke fortrolige oplysninger. Eksempelvis: væsentlige sociale forhold] |  |  |  |

## Behandlingens omfang

*Her skal du beskrive omfanget af behandlingen, herunder navnlig følgende oplysninger:
- Hvor mange personoplysninger behandles (omfanget af behandlingen af personoplysninger samt detaljeringsgrad, dvs. evne til at identificere borgerne)?
- Hvor mange personer behandles der oplysninger om (antallet af borgere, stort antal, mindre antal)?
- Hvor ofte foretages der behandling af personoplysninger (behandlingens frekvens, dvs. om behandlingen er enkeltstående, regelmæssig, kontinuerlig etc.)?
- Hvor længe behandles der personoplysninger (tidsmæssig udstrækning)?
- Hvilke geografiske områder dækker behandlingen (geografisk udstrækning, herunder lokalt, regionalt, nationalt, internationalt, globalt)?*

# 4. Lovlighed, nødvendighed og proportionalitet

## Hjemmel til behandling af personoplysningerne

*Hvilket retligt grundlag (hjemmel) har behandlingen (f.eks. samtykke, kontraktforhold, retlig forpligtelse (hvilken?), offentlig myndighedsudøvelse og særlovgivning)?*

## Princippet om rimelighed og gennemsigtighed

*Beskriv, hvordan det sikres, at personoplysningerne behandles lovligt, rimeligt og på en gennemsigtig måde i forhold til borgerne
- Hvis samtykke: Indsamles der et gyldigt samtykke, der kan dokumenteres over tid?
- Hvordan indhentes eventuelle samtykker fra borgerne?
- Er det lige så enkelt at trække samtykket tilbage, som det er at give det?
 - Overvej, om der er hjemmel til både indsamlingen og en eventuel videregivelse af personoplysningerne?
- Foretages der særlige behandlingsformer, der har særlige hjemmelskrav, f.eks. profilering, biometri, samkøring i kontroløjemed, fuldautomatiske afgørelser, markedsføring m.v.?
- Hvordan varetages åbenhed (transparens) i behandlingen?]*

Forslag til tekst (skal rettes til):
Det fremgår af databeskyttelsesforordningens artikel 5, stk. 1, litra a, at personoplysninger skal behandles lovligt, rimeligt og på en gennemsigtig måde i forhold til den registrerede.

For så vidt angår kravet om lovlighed henvises til afsnittet ovenfor, der indeholder en beskrivelse af Fredensborg Kommunens hjemmelsgrundlag ved behandling af personoplysninger i forbindelse med [projektet//behandlingen].

[Beskrivelse af rimelighed, f.eks. hvordan det sikres, at der ikke sker forskelsbehandling samt den registreredes egen interesse i behandlingen og oplysning herom.]

I kravet om gennemsigtighed ligger, at det bør være gennemsigtigt for de pågældende fysiske personer, at personoplysninger, der vedrører dem, indsamles, anvendes, tilgås eller på anden vis behandles, og i hvilket omfang personoplysningerne behandles eller vil blive behandlet.

[Beskrivelse af, hvad de registrerede evt. gøres opmærksom på/oplyses om, ud over privatlivspolitikken.]

Fredensborg Kommune oplyser de registrerede om behandlingen af personoplysninger, herunder formålene med behandlingen, på en lettilgængelig og letforståelig måde. For nærmere herom se om oplysningspligten nedenfor.

Fredensborg Kommune har desuden interne retningslinjer og procedurer for håndtering af anmodninger om indsigt fra registrerede.

Det vurderes på baggrund af ovenstående, at Fredensborg Kommune lever op til kravet om lovlighed, rimelighed og gennemsigtighed ved behandlingen af personoplysninger i forbindelse med [projektet/behandlingen].

## Princippet om formålsbegrænsning

*Beskriv, hvordan det sikres, at personoplysningerne indsamles til udtrykkeligt angivne og legitime formål og ikke viderebehandles på en måde, der er uforenelig med disse formål.
- Er formålet klart defineret og specifikt?
- Er formålet sagligt?
- Sker der viderebehandling af personoplysningerne til nye formål?
- Kan formålet opnås med en mindre indgribende behandling?*

Forslag til tekst (skal rettes til):
Personoplysninger skal indsamles til udtrykkeligt angivne og legitime formål og må ikke viderebehandles på en måde, der er uforenelig med disse formål (”formålsbegrænsning”), jf. databeskyttelsesforordningens artikel 5, stk. 1, litra b, 1. led.

Som nærmere beskrevet i afsnit 3, er formålet med Fredensborg Kommunes behandling af personoplysninger […].

Kommunen påtænker ikke at viderebehandle de personoplysninger, der indsamles i forbindelse med [projektet/behandlingen], til andre formål end de netop angivne. Såfremt en sådan viderebehandling måtte blive aktuel, vil der ske en revidering af denne konsekvensanalyse.

Eventuelt: Personoplysninger, der indsamles og behandles i forbindelse med [projektet/behandlingen], kan dog efterfølgende blive anvendt til forskning efter reglerne i databeskyttelseslovens § 10. I så fald behandles disse oplysninger alene med henblik på at udføre statistiske eller videnskabelige undersøgelser af væsentlig samfundsmæssig betydning, og kun i det omfang behandlingen er nødvendig for undersøgelsen.

Sammenfattende vurderes det, at behandlingen af personoplysninger i forbindelse med [projektet/behandlingen] sker til udtrykkeligt angivne og legitime formål, samt at personoplysninger ikke viderebehandles på en måde, der er uforenelig med disse formål.

## Princippet om dataminimering

*Beskriv hvordan det sikres, at personoplysningerne er tilstrækkelige, relevante og begrænset til, hvad der er nødvendigt i forhold til de formål, hvortil de behandles.
- Kan formålet opnås ved at begrænse – eventuelt helt at undgå – behandlingen af personoplysninger?
- Kan formålet opnås ved brug af anonymiserede, aggregerede eller pseudonymiserede oplysninger?
- Kan formålet opnås ved at behandle mindre detaljerede personoplysninger?
- Kan det undgås at behandle følsomme personoplysninger eller oplysninger om strafbare forhold?
- Nødvendigheden bør beskrives for behandlingen for hvert enkelt formål.*

Forslag til tekst (skal rettes):
Personoplysninger skal være tilstrækkelige, relevante og begrænset til, hvad der er nødvendigt i forhold til de formål, hvortil de behandles (”dataminimering”), jf. databeskyttelsesforordningens artikel 5, stk. 1, litra c.
Ved vurderingen af behandlingens nødvendighed må der overordnet set lægges vægt på, at [beskriv nødvendigheden af behandlingen]. Fredensborg Kommune indsamler alene de oplysninger, der er nødvendige for, at kommunen kan [beskriv behandlingen].

Fredensborg Kommunes behandling af personoplysninger i forbindelse med [projektet/behandlingen] vurderes på denne baggrund ikke at overstige, hvad der er nødvendigt. Kommunen kan ikke opnå det overordnede formål med [projektet/behandlingen], såfremt personoplysningerne anonymiseres eller aggregeres.

Sammenfattende vurderes det, at behandlingen af personoplysninger i forbindelse med
[projektet/behandlingen] er tilstrækkelig, relevant og begrænset til, hvad der er nødvendigt i forhold til de formål, hvortil oplysningerne behandles.

## Princippet om rigtighed

*Beskriv, hvordan det sikres, at personoplysningerne er korrekte og om nødvendigt ajourførte.
- Hvordan sikres det, at personoplysningerne er korrekte, når de indsamles (datavalidering)?
- Hvordan sikres det, at personoplysningerne forbliver korrekte under behandlingen, herunder kontrol heraf?
- Hvordan sikres det, at personoplysninger kan berigtiges og slettes, herunder ved brug af tekniske funktioner, automatiske og manuelle procedurer?
- Hvordan kan borgernes anmodninger om berigtigelse og sletning håndteres?
- Er der overblik over, hvem personoplysningerne deles med, således at eventuelle modtagere kan underrettes i tilfælde af registrering af urigtige personoplysninger?*

Forslag til tekst (skal rettes til):
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 (”rigtighed”), jf. databeskyttelsesforordningens artikel 5, stk. 1, litra d.

Det er væsentligt, at personoplysningerne om de registrerede, er korrekte, og at der sker den fornødne verifikation, således at [uddyb hvilken betydning det har].

Hvis oplysningerne ikke er korrekte, vil dette hindre formålet med [projektet/behandlingen]. [Indsæt overordnet beskrivelse af foranstaltninger, der sikrer datakvalitet, datavalidering m.v.].

Sammenfattende vurderes det, at de personoplysninger, der behandles i forbindelse med [projektet/behandlingen], er korrekte og ajourførte, ligesom det vurderes, at der også er mulighed herfor.

## Princip om opbevaringsbegrænsning

*Beskriv, hvordan det sikres, at personoplysningerne opbevares på en sådan måde, at det ikke er muligt at identificere borgerne i et længere tidsrum end det, der er nødvendigt til de formål, hvortil de pågældende personoplysninger er indsamlet.
- Hvad er den nødvendige opbevaringsperiode for hvert enkelt formål, som behandlingen forfølger?
- Foretages der fortsat behandling af personoplysninger, efter at formålet med behandlingen er opnået?
- Kan formålet med behandlingen opnås ved en kortere opbevaringsperiode?
- Kan der foretages en effektiv sletning eller anonymisering, herunder backup og logs?
- Hvordan sikres det, at personoplysninger slettes eller anonymiseres effektivt alle de steder, hvor de opbevares, herunder på lokale og bærbare opbevaringsmedier, f.eks. computer og telefon?
- Hvordan understøtter de implicerede systemer rent teknisk muligheden for angivelse af et tidspunkt for sletning som funktion af afgørende faktorer?
- Beskrivelse af de i opbevaringsmedierne og systemerne implementerede procedurer for automatisk sletning af personoplysninger.
- Beskrivelse af proceduren for manuel sletning af de implicerede opbevaringsmedier og systemer, herunder proceduren for autorisation af personale til at udføre den manuelle sletning.
- Beskrivelse af proceduren for opfølgning på sletning, herunder (1) hvordan det sikres, at en given oplysning er slettet i alle de berørte systemer/medier, (2) hvordan det kontrolleres, at oplysninger er slettet inden for de fastlagte frister, og (3) hvordan det kontrolleres, at oplysninger indgivet til manuel sletning er blevet udført rettidigt.
- Beskrivelse af, hvordan logning over sletning foretages.
- Beskrivelse af proceduren for sletning i forbindelse med backups af databaser, herunder (1) hvordan det sikres, at slettede oplysninger ikke gendannes i forbindelse med genindlæsning fra tidligere backups, samt (2) hvordan det sikres, at integriteten af eventuelle logs over sletningskørsler, som skal genkøres efter genindlæsning af tidligere backups, bevares.*

Forslag til tekst (skal rettes til):
Efter princippet om opbevaringsbegrænsning i databeskyttelsesforordningens artikel 5, stk. 1, litra e, skal personoplysninger 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. Personoplysninger indsamles i forbindelse med [projektet/behandlingen], som beskrevet ovenfor, og opbevares i systemet [systemnavn] i en periode på op til [… uger/måneder/år] i overensstemmelse med [angiv regler].

## Princippet om fortrolighed og integritet

*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. Behandlingssikkerhed er endvidere nærmere reguleret i GDPR, der stiller krav om, at kommunen udarbejder en risikovurdering af behandlingssikkerheden. Beskriv, hvordan kravene til behandlingssikkerheden overholdes.
- Hvordan fungerer de forskellige systemer/applikationer, der skal foretage behandlingen, herunder disses eventuelle indbyggede sikkerhedsforanstaltninger?
- Hvad er resultatet af den udarbejdede risikovurdering vedrørende behandlingssikkerhed?*

Forslag til tekst (skal rettes):
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 (”integritet og fortrolighed”). Hertil kommer, at kommunen skal fastsætte passende sikkerhedsforanstaltninger efter en risikovurdering i overensstemmelse med databeskyttelsesforordningens artikel 32 om behandlingssikkerhed.

Behandlingen af personoplysninger i forbindelse med [projektet/behandlingen] foregår [beskriv system e.l.,
hvor behandlingen foregår, herunder hvis det sker på tværs af en række forskellige systemkomponenter].

Forhold vedrørende behandlingssikkerhed er beskrevet i risikovurderingen vedrørende behandlingssikkerhed (bilag […]), hvortil der henvises.

## Privacy by design

*Beskriv, hvordan kommunen har indrettet sig teknisk og organisatorisk med henblik på at opnå effektiv implementering af databeskyttelsesreglerne.
- Hvilke tekniske foranstaltninger er der truffet?
- Hvilke organisatoriske foranstaltninger er der truffet?
- Er foranstaltningerne implementeret?
- Er der udarbejdet et kravkatalog over tekniske, funktionelle og non-funktionelle krav vedrørende databeskyttelse til løsningen, f.eks. et nyt sagsbehandlingssystem, sundhedsapp etc.?*

Forslag til tekst (skal rettes):

Databeskyttelsesforordningens artikel 25 stiller krav til, hvordan Fredensborg Kommune skal indrette sig teknisk og organisatorisk for at opnå effektiv implementering af databeskyttelsesreglerne på en dokumenterbar måde. Artikel 25 skal ses i sammenhæng med forordningens øvrige bestemmelser, herunder navnlig principperne for behandling i artikel 5, den Kommunens pligter i artikel 24 og kravene til
behandlingssikkerhed i artikel 32.

Forordningens artikel 25 indebærer, at der for behandlingen som helhed skal træffes både tekniske og organisatoriske foranstaltninger. Der er imidlertid ikke krav om, at der træffes både tekniske og
organisatoriske foranstaltninger for hvert enkelt delelement i behandlingen.

Det følger af artikel 25, stk. 1, at de tekniske og organisatoriske foranstaltninger skal være designet med henblik på effektiv implementering af databeskyttelsesprincipper og med henblik på integrering af de fornødne garantier i behandlingen af personoplysninger for at opfylde kravene i forordningen og beskytte de registreredes rettigheder. Dette skal ske under hensyntagen til det aktuelle tekniske niveau,
implementeringsomkostningerne og den pågældende behandlings formål, karakter, sammenhæng og
omfang samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og
frihedsrettigheder, som behandlingen indebærer. Fastlæggelsen af de nødvendige foranstaltninger skal
både foretages på tidspunktet for fastlæggelse af midlerne til behandlingen og på tidspunktet for selve
behandlingen.

[Beskrivelse af om det er indtænkt i system/ved udvikling af system.]

Af forordningens artikel 25, stk. 2, fremgår desuden, at den Kommunen skal 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.

Fredensborg Kommune tager løbende stilling til, hvilke personoplysninger der er nødvendige at indsamle og
behandle i forbindelse med [projektet/behandlingen]. Dette sikres også gennem interne retningslinjer og
undervisning af ansatte samt vejledning til de registrerede.

Kommunen sikrer gennem fastsatte slettefrister og sletteprocedurer, at personoplysninger slettes i overensstemmelse med princippet om opbevaringsbegrænsning (se afsnit 5.5 ovenfor).

Adgangen til personoplysninger begrænses via Fredensborg Kommunes interne procedurer for adgangsstyring samt krav til sikkerhed i systemet (se afsnit 5.7 vedr. behandlingssikkerhed).

[Kommunen har endvidere ved udviklingen af systemet indtænkt databeskyttelse i løsningsdesignet, hvilket er dokumenteret i vedlagte kravkatalog over tekniske, funktionelle og non-funktionelle krav vedrørende databeskyttelse til løsningen.]

## Oplysningspligten

*Beskriv, hvordan det sikres, at oplysningspligten i forordningens artikel 13 og 14 overholdes, herunder hvis der sker genanvendelse af personoplysninger til nye formål, og hvis der er personoplysninger/behandlinger, som vurderes undtaget fra oplysningspligten, jf. databeskyttelsesforordningens artikel 14, stk. 5 og databeskyttelseslovens § 22.*

Forslag til tekst (skal rettes):

Det følger af reglerne om oplysningspligt i databeskyttelsesforordningens artikel 13 og 14, at de registrerede som udgangspunkt skal underrettes om Fredensborg Kommunes behandling af personoplysninger.

Fredensborg Kommune behandler både personoplysninger, der er indsamlet fra den registrerede selv, og
personoplysninger, der er indsamlet fra andre end den registrerede – f.eks. fra [Indsæt hvor oplysningerne kan blive indsamlet fra] .

Kommunen er derfor både omfattet af forordningens artikel 13 og 14.

Personoplysninger som den registrerede selv oplyser, omfattes af forordningens artikel 13. Kommunen informerer den pågældende om behandlingen af personoplysninger ved [indsæt beskrivelse].

Personoplysninger som Fredensborg Kommune modtager fra […], omfattes af forordningens artikel 14. Kommunen informerer den pågældende om behandlingen af personoplysninger ved [indsæt beskrivelse].

Hvis relevant ved undtagelse til oplysningspligten: For så vidt angår personoplysninger om modtaget fra [indsæt hvem oplysningerne modtages fra], kan Fredensborg Kommune gøre undtagelse fra oplysningspligten efter [forordningens artikel 14, stk. 5, litra […]/databeskyttelseslovens § 22, stk. […]]. Efter bestemmelsen finder oplysningspligten ikke anvendelse, da [beskriv undtagelse og situation].

I sådanne tilfælde træffer Fredensborg Kommune passende foranstaltninger for at beskytte den registreredes rettigheder og frihedsrettigheder samt legitime interesser.
Fredensborg Kommune har ved denne vurdering navnlig lagt vægt på, at [uddyb, f.eks. forholdene, typen af
personoplysninger, hvordan de indsamles, antallet af registrerede, muligheden for at opfylde oplysningspligten, f.eks. hvor e-mailadresse eller postadresse ikke haves samt hvorvidt personoplysningerne er gjort tilgængelige andetsteds].

## Øvrige rettigheder

*Beskriv, hvordan det sikres, at de øvrige rettigheder i artikel 15, 16, 17, 18, 20 og 21 overholdes. Bemærk, at der i nogle tilfælde gælder begrænsninger ift. disse rettigheder. Nedenfor er indsat et forslag til tekst, der dog skal tilrettes og uddybes for den enkelte konsekvensanalyse, herunder særligt ift. interne retningslinjer.*

Forslag til tekst (skal rettes):

De registrerede oplyses om deres øvrige rettigheder efter databeskyttelsesforordningens kapitel III i
forbindelse med Fredensborg kommunes iagttagelse af oplysningspligt efter forordningens artikel 13 og 14 (se ovenfor). Disse rettigheder omfatter […].

[Hvor det er relevant: Retten til […] er derimod undtaget, idet […]].

Fredensborg Kommune foretager [ikke] automatiske individuelle afgørelser omfattet af databeskyttelsesforordningens artikel 22 i forbindelse med [projektet/behandlingsaktiviteten].

[Hvis § 22 er relevant, uddybes det her].

Fredensborg Kommune håndterer løbende rettighedsanmodninger fra de registrerede og sikrer, at
databeskyttelsesforordningens krav til håndtering af rettighedsanmodninger efterleves. Til brug herfor har
den Kommunen udarbejdet interne retningslinjer og procedurer for håndtering af rettighedsanmodninger.

# 5. Databehandlere, videregivelse og tredjelandsoverførsler

## Forholdet til databehandlere

 *Her anføres det, hvordan det sikres, at eventuelle databehandlere og underdatabehandlere overholder de databeskyttelsesretlige regler:
- Anvendes der databehandlere til behandlingen?
- Anvendes der underdatabehandlere til behandlingen?
- Hvordan sikres det, at databehandlere og underdatabehandlere overholder kravene til databehandlere i forordningen?
- Hvordan sikres det, at kommunen fører fornødent tilsyn med databehandlere og underdatabehandlere, herunder at de overholder reglerne om bl.a. sikkerhedsforanstaltninger, samt at de ikke anvender personoplysningerne til egne formål eller overfører personoplysninger uretmæssigt til tredjelande eller tredjeparter?
- Anvendes der cloudleverandører, og hvordan føres der i så fald tilsyn med disse og opnås overblik over databehandlingen?*

Forslag til tekst (skal rettes):

Som beskrevet ovenfor er Fredensborg Kommune ansvarlig for den behandling af personoplysninger, der foretages som led i [projektet/behandlingen].

Fredensborg Kommune har indgået en databehandleraftale med [leverandøren/leverandører] vedrørende behandlingen af personoplysninger i forbindelse med [projektet/behandlingen].

Hvis der også er underdatabehandlere: Der er endvidere indgået en underdatabehandleraftale mellem [databehandler] og (underdatabehandler(e)] vedrørende [fx driften] heraf. For nærmere om dette set-up se beskrivelsen i bilag […].

Alle aftalerne indeholder bestemmelser om tilsyn, bistand til Fredensborg Kommune, underretning af kommunen i tilfælde af brud m.v. Aftalerne er baseret på Datatilsynets skabeloner samt kommunens risikovurderinger af databehandlernes behandlinger.

## Videregivelse af personoplysninger

*Her angives hvilke modtagere, personoplysningerne videregives til (selvstændig dataansvarlig), hvis de videregives.*

## Overførsel af personoplysninger til modtagere i tredjelande og internationale organisationer

*Her skal du beskrive, hvordan det sikres, at der alene sker eventuel overførsel af personoplysninger til modtagere i tredjelande eller internationale organisationer i overensstemmelse med reglerne om internationale overførsler af personoplysninger i GDPR.*

*- Overføres der personoplysninger til modtagere i tredjelande eller internationale organisationer – eventuelt gennem databehandlere eller underdatabehandlere?*

*- Overføres der til et sikkert tredjeland (hvor der er en positiv afgørelse om tilstrækkeligheden af beskyttelsesniveauet) eller usikkert tredjeland?*

*- Hvad er overførselsgrundlaget, f.eks. EU-Kommissionens standardkontraktbestemmelser?*

*- Hvilke sikkerhedsforanstaltninger tages i den forbindelse?*

*- Hvis der overføres personoplysninger til usikre tredjelande, er der så udarbejdet en Transfer Impact Assessment (TIA) med henblik på at vurdere overførslens lovlighed, herunder behovet for at fastsætte supplerende foranstaltninger?*

*- Er behandlingen omfattet af lokationskravet (tidligere ”krigsreglen”) i databeskyttelsesloven?*

Forslag til tekst (skal rettes):
Hvis der ikke sker overførsel: Det er for nuværende ikke hensigten, at personoplysningerne vil blive overført til tredjelande eller internationale organisationer. Såfremt en sådan overførsel til tredjelande eller internationale organisationer måtte blive aktuelt, vil der ske en revidering af denne konsekvensanalyse med henblik på forudgående at sikre det fornødne lovlige overførselsgrundlag samt hjemmelsgrundlag for overførslen, samt at den i øvrigt vil ske på en sikkerhedsmæssig forsvarlig måde.

Der er i samtlige databehandleraftaler indskrevet, at der ikke må ske overførsel af personoplysninger til
tredjelande eller internationale organisationer, og at personoplysninger ikke må tilgås af personer uden for
EU/EØS.

# 6. Risici samt foranstaltninger

## Valg af evalueringskriterier for konsekvens og sandsynlighed

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:

*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*



## 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).*

# 7. Konklusion og ledelsesgodkendelse

## [Projektets/behandlingens] samlede restrisiko 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 projektet/behandlingen.*

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 påbegyndes. Det skal fremgå her, om der skal ske høring af Datatilsynet.*

Forslag til tekst:

Fredensborg Kommune har pligt til at foretage en forudgående høring af Datatilsynet, inden påbegyndelsen af en påtænkt behandling af personoplysninger, hvis konsekvensanalysen viser, at behandlingen vil føre til en høj risiko, og kommunen ikke kan begrænse denne høje risiko ved indførelse af passende
foranstaltninger, jf. databeskyttelsesforordningens artikel 36.

Som det fremgår ovenfor, er det Fredensborg Kommunes vurdering, at den samlede residualrisiko –
dvs. risikobilledet efter indførelse af foranstaltninger til at imødegå de identificerede risici – er [indsæt risiko].

Det er på denne baggrund, at Fredensborg Kommune har hørt Datatilsynet. [Datatilsynets eventuelle
bemærkninger.] / Det er på denne baggrund, at Fredensborg Kommune har vurderet, at det ikke er nødvendigt at høre Datatilsynet i forbindelse med [projektet/behandlingen].

## Ledelsens godkendelse af konsekvensanalysen

|  |  |  |
| --- | --- | --- |
| [ ]  | Godkendt | Behandlingsaktiviteten kan påbegyndes, hvis de afhjælpende foranstaltninger i handlingsplanen 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 godkendelsen er følgende:

[Indsæt begrundelse]

## Bilag til konsekvensanalysen

Følgende bilag vedlægges 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

[ ]  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

[ ]  Andre:

## Ajourføring af konsekvensanalysen

Fredensborg Kommune 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.]