Retningslinjer for databehandleraftaler og tilsyn

Revisionshistorik

Version	Dato	Beskrivelse af ændringer	Udført af	Godkendt af
2.2	23-08-2022	Mindre redaktionelle rettelser samt tilføjelse af afsnit om tredjelandsoverførsler	Sikkerhedsrådgiver	Sikkerhedsteam
2.3	07-09-2023	Tilføjelse af afsnit vedr. fortrolighedserklæringer samt uddybning af tilsynsproces, vurdering af behov for konsekvensanalyse og afsnit om risikovurdering	Sikkerhedsrådgiver	Sikkerhedsteam
3	19-11-2024	Flere større ændringer foretaget, bl.a. uddybning af konsekvensanalyse-afsnit samt tilføjelse af DBS' tilsyn	Sikkerhedsrådgiver	Sikkerhedsteam

Indhold

Formål og anvendelsesområde

Formålet med retningslinjerne er at sikre, at Jammerbugt Kommune vurderer placering af dataansvar korrekt, at der indgås databehandleraftaler med databehandlere og underdatabehandlere, og at der føres tilsyn med disse. Retningslinjerne skal være med til at understøtte, at kommunens aftaler bidrager til at sikre, at de personoplysninger, som kommunen indsamler til udtrykkeligt angivne og legitime formål, ikke viderebehandles på en måde, der er uforenelig med disse formål.

Systemejere og ledere, som har hhv. systemansvar eller anvender leverandører af services (konsulenthuse mv.), kan anvende retningslinjerne som instruks.

Ved systemejere forstås ledere, som har ansvaret for et eller flere it-systemer, jf. definitionen i kommunens informations- og it-sikkerhedspolitik.

Ved ledere, der anvender leverandører af services, forstås ledere med ansvaret for en aftale med et eksternt firma om behandling af kommunens data, fx et konsulenthus, leverandører af hjemme- og sygepleje, vikarer mv. Den eksterne leverandør kan enten behandle data i kommunens it-systemer eller behandle data, som kommunen overlader til dem. Lederne, hvis afdeling har indgået aftale/kontrakt med leverandøren herom, har således ansvaret for, at der indgås en databehandleraftale, og at der tilrettelægges tilsyn med databehandleren.

Afklaring af dataansvar

Ved alle behandlinger af personoplysninger foreligger der et dataansvar. En behandling kan omfatte enhver håndtering af personoplysninger herunder:

Indsamling, registrering, organisering, systematisering, opbevaring, tilpasning eller ændring, genfinding, søgning, brug, videregivelse ved transmission, formidling eller enhver anden form for overladelse, sammenstilling eller samkøring, begrænsning, sletning eller tilintetgørelse.

Inden en behandling af personoplysninger påbegyndes, er det vigtigt indledningsvist at afklare placeringen af dataansvaret, fordi kravene til en dataansvarlig og en databehandler er forskellige. Hvis de parter, der deltager i en behandling af personoplysninger, er usikre på, hvem der har ansvaret for at leve op til de forskellige regler om databeskyttelse, er der en risiko for, at ingen af parterne påtager sig ansvaret, eller at en part påtager sig et ansvar, som den pågældende reelt ikke har. Det er derfor vigtigt, at Jammerbugt Kommune – inden kommunen begynder at behandle personoplysninger – får afklaret, hvilken rolle kommunen og eventuelle andre parter har i forbindelse med behandlingen.

Det skal således først afklares, hvorvidt kommunen er dataansvarlig, databehandler, eller om der forelægger et fælles dataansvar. Vurderingen foretages af sikkerhedsrådgiveren og evt. DPO'en, hvis det er relevant i den pågældende sammenhæng. Til hjælp kan nedenstående rolledefinitioner anvendes:

Dataansvarlig/dataejer

- Den dataansvarlig afgør, hvorfor (med hvilket formål) og hvordan (med hvilke hjælpemidler) personoplysningerne behandles.

Databehandler

- En databehandler kendetegnes ved at behandle personoplysninger på vegne af (efter instruks fra) en dataansvarlig.
- Databehandleren behandler således aldrig personoplysninger til egne formål og må derfor ikke bruge de overladte oplysninger til andet end udførelsen af opgaven for den dataansvarlige.

Fælles dataansvar

- Fælles dataansvar mellem to eller flere parter kan komme på tale, hvis parterne i fællesskab bestemmer, hvorfor der skal behandles personoplysninger (formålet), og hvordan der skal behandles personoplysninger (hjælpemidlerne).
- Et fælles dataansvar kan komme på tale, hvis part 1 og part 2 sammen har ansvaret for en behandling, og hvis de begge har ret til at bruge oplysningerne til egne formål. Der er altså ikke tale om et fælles dataansvar, hvis en behandling kun foretages til den ene parts formål.

Det er vigtigt at bemærke, at det ikke er i alle tilfælde, at en aftale mellem to parter betyder, at den ene har rollen som databehandler – altså at der er en databehandlerkonstruktion. For at der er tale om en databehandlerkonstruktion, skal aftalen mellem de to parter først og fremmest dreje sig om behandling (indsamling, opbevaring, sletning mv.) af personoplysninger – og ikke eksempelvis være en håndværksydelse.

Log-in-oplysninger
Kommunens DPO har vurderet, at det ikke er relevant at indgå databehandleraftaler ved systemer, hvor der udelukkende behandles personoplysninger via login, dvs. brugernavn og adgangskode. Heller ikke selvom et brugernavn udgør personoplysninger fx i form af et CPR.nr. eller et UNI-login. Dette skyldes, at formålet med databehandlingen ikke er at behandle personoplysninger om fysiske personer. Loginet er nærmere en hjælpemiddel, som leverandøren vælger at tage i brug for at sikre, at kun de rette vedkommende får adgang til løsningen, dvs. en behandling til egne formål.

Det forudsætter imidlertid, at der ikke i systemet behandles øvrige former for personoplysninger, som tilkobles brugeren, fx opgavebesvarelser eller status på gennemførsel af kurser. I så fald vil der være tale om en databehandlerkonstruktion.

Fortrolighedserklæring

I nogle tilfælde benytter kommunen leverandører, som ikke agerer som databehandlere, men som kan få adgang til de personoplysninger eller fortrolige/følsomme forretningsoplysninger, der opbevares i kommunens it-systemer eller fysisk på kommunens lokationer. Det kan fx være servicepersonale som rengøring eller it-leverandører, som udfører tekniske driftsopgaver i kommunens it-infrastruktur.

Det kan ske, at medarbejdere ansat hos disse leverandører kan få adgang til førnævnte oplysninger, hvorfor Jammerbugt Kommune altid indgår tavsheds- og fortrolighedserklæring med leverandøren. Der anvendes en fast skabelon til erklæringer, som forefindes på Tryk.

Risikovurdering og konsekvensanalyse

I Jammerbugt Kommune har systemejere ansvar for at udarbejde risikovurderinger af samtlige it-systemer, hvori personlysninger behandles, og derudover vurderer systemejere gennem risikovurderingen behovet for eventuelt at udarbejde en supplerende konsekvensanalyse. Det samme gælder for ledere, der anvender leverandører, som behandler personoplysninger på vegne af kommunen.

Risikovurdering

Det er et krav, at der udarbejdes risikovurderinger for kommunens behandlingsaktiviteter. Lederen, som er noteret som ansvarlig for den pågældende behandlingsaktivitet, jf. kommunens fortegnelser over behandlingsaktiviteter, er ansvarlig for at udarbejde risikovurderingen samt årligt revidere den.

Der er krav om, at systemejer udarbejder risikovurderinger for alle systemer, som behandler personoplysninger. Ligeledes er det et krav, at systemejer reviderer risikovurderinger årligt for at sikre, at vurderingen er opdateret og ajourført i forhold til det gældende sikkerheds- og trusselsniveau.

I tilfælde af en ny databehandling skal kommunen, allerede før en behandling påbegyndes, udarbejde en kortlægning af risici for de registreredes rettigheder og en afvejning af disse risici i forhold til de forholdsregler, der bliver truffet for at beskytte disse rettigheder. Det vil sige, at systemejer eller ledere inden ibrugtagning af et nyt system, der behandler personoplysninger, eller opstart af en ny proces/arbejdsgang, hvori behandlingen af personoplysninger indgår, skal udarbejde en risikovurdering.

Selve risikovurderingen består af flere dele:

- En kortlægning af alle de risici/trusler, behandlingen medfører, og en kategorisering (risikoscoring af sandsynlighed og konsekvens) heraf. Risici kan fx være manglende adgangsstyring eller it-angreb.
- En beskrivelse af relevante organisatoriske og tekniske sikkerhedsforanstaltninger, samt en vurdering af, om sikkerheden vurderes tilstrækkelig.

- En handleplan eller opgaveliste, som adresserer trusler med høje og eller middel risikoscorer, herunder hvorvidt risici accepteres eller mitigeres ved at iværksætte yderligere sikkerhedsforanstaltninger

Til udarbejdelse af risikovurderinger anvendes kommunens skabelon, som findes på Tryk.

Konsekvensanalyse
En konsekvensanalyse (også kaldet DPIA) er en proces, der har til formål at vurdere risici for fysiske personers rettigheder og frihedsrettigheder og fastlægge foranstaltninger til at afhjælpe disse risici. Analysen skal således beskrive, hvilken behandling der foretages, vurdere behandlingens nødvendighed og proportionalitet samt bidrage til at håndtere de risici, som behandlingen af personoplysninger medfører.

Ansvaret for processen for udarbejdelse af konsekvensanalyser er primært placeret decentralt. Udarbejdelsen skal ske med rådgivning og inddragelse fra ledelse, centrale personer og DPO.

Hvornår skal der udarbejdes en konsekvensanalyse?
Konsekvensanalysen skal foretages forud for, at behandlingen påbegyndes, og analysen skal ses som et redskab til at hjælpe beslutningsprocessen vedrørende behandlingen. Der skal udarbejdes en konsekvensanalyse, hvis kommunen vurderer, at behandlingen af personoplysninger udgør **en høj risiko for den registrerede**. Det kan være i form af høje risici, som er kommet frem i risikovurderingen, eller høje risikotilfælde, som vil udløse et behov for at udarbejde en konsekvensanalyse.

Høje risici
Kommunen vil i risikovurderinger vurdere, hvilke behandlinger af data som kan medføre høje risici for de registrerede. I de tilfælde, hvor risikoen ikke kan nedbringes eller mitigeres til et passende niveau, vil kommunen som udgangspunkt skulle udarbejde en konsekvensanalyse. Kommunen vil desuden udarbejde konsekvensanalyser i de tilfælde, hvor der i risikovurderingen konstateres en høj konsekvens uagtet af, hvordan sandsynligheden vurderes.

Kommunen lægger i forbindelse med konsekvensvurderingen vægt på følgende faktorer:

Omfanget af databehandlingen
Der er ikke for nuværende defineret, hvad et stort omfang af databehandling omfatter. Kommunen vil vurdere, hvorvidt en databehandling omfatter 'stort omfang' ud fra en eller flere af følgende faktorer:

- Behandling af over 500 registreredes oplysninger
- Mængden af data og/eller de forskellige data, der behandles, fx hvis der behandles omfattende mængde almindelige personoplysninger på registrerede, selvom der er tale om få registrerede
- Databehandlingens varighed eller regelmæssighed
- Databehandlingens geografiske omfang

Typen af registrerede
Behandlingen af sårbare personers personoplysninger kan ofte medføre, at enkeltpersoner kan være ude af stand til på en nem måde at give deres samtykke til eller modsætte sig behandlingen af deres oplysninger eller udøve deres rettigheder.

Sårbare registrerede defineres i kommunen som værende børn (de kan betragtes som værende ude af stand til bevidst og med omtanke at modsætte sig eller give deres samtykke til behandling af deres data), ansatte, mere sårbare udsnit af befolkningen med behov for særlig beskyttelse (psykisk syge personer, asylansøgere, ældre, patienter osv.), og i tilfælde, hvor der kan konstateres ubalance i forholdet mellem den registreredes og den dataansvarliges position.

Det vil sige, at databehandlinger, hvor sårbare personers oplysninger behandles i stort omfang, som udgangspunkt vil udløse et behov for udarbejdelse af en konsekvensanalyse.

Høje risikotilfælde
Høje risikotilfælde (også kaldet iboende høje risici) defineres som:

1. Behandling af biometriske data med det formål entydigt at identificere en fysisk person.
2. Behandling af genetiske data.
3. Behandling af lokationsdata i sammenhæng med mindst et yderligere kriterie fra Artikel 29-gruppens retningslinjer (WP248 rev. 01).
4. Behandling ved brug af nye teknologier, fx cloud-services, applikationer med borgerkontakt, kunstig intelligens, brug af elektroniske identiteter mv. Behandling, der fører til afgørelser om en fysisk persons rettigheder til et produkt, en service, en potentiel mulighed eller begunstigelse, der er baseret på en hvilken som helst form for automatiseret afgørelse (herunder profilering)
5. Behandling, der omfatter profilering af fysiske personer i stor skala
6. Behandling af personoplysninger om sårbare personer (se definition i forrige afsnit 'Typen af registrerede'), eller hvor der er tale om behandling af følsomme oplysninger (særlige kategorier), og hvor der benyttes profilering eller andre former for automatiserede afgørelser
7. Behandlinger, hvor et brud på persondatasikkerheden kan have en direkte effekt på en persons fysiske helbred eller på sikkerheden for en fysisk person.

Ovenstående liste er ikke udtømmende, og der kan derfor være yderligere tilfælde, hvor kommunen vurderer, at databehandlingen medvirker til en høj iboende risiko for de registrerede.

Der skal altid udarbejdes en risikovurdering forud for en konsekvensanalyse, da en konsekvensanalyse har til formål nærmere at beskrive præcis de steder, som indebærer en høj risiko for de registrerede. Behandlingsaktiviteterne skal altid beskrives grundigt i konsekvensanalysen, fx i forhold til formålet med databehandlingen og overholdelse af de registreredes rettigheder. I selve analysedelen vil kommunen vurdere de høje risici herunder

høje iboende risici og/eller de høje risikotilfælde, som udløste behovet for konsekvensanalysen.

Screening af behov for konsekvensanalyse
Når kommunen skal vurdere, om der er behov for at udarbejde en konsekvensanalyse for en given databehandling, er der tale om en konkret vurdering fra gang til gang. Det er systemejerens opgave (eller dennes forvalter) at screene it-systemer for, hvorvidt der kan være behov for at udarbejde en konsekvensanalyse. Dette gøres gennem udfyldelse af kommunens skabelon til risikovurderinger, hvor der fremgår en metode til screening som en del af risikovurderingen.

Hvis screeningen viser, at der enten skal eller at der muligvis skal udarbejdes en konsekvensanalyse, skal systemejer eller dennes forvalter kontakte sikkerhedsrådgiveren for at få en endelig vurdering af behovet for udarbejdelse af en konsekvensanalyse og evt. igangsat en proces for udarbejdelse af konsekvensanalysen. Beslutningen vil blive foretaget på baggrund af en samlet vurdering af, hvorvidt der er høje risici og/eller høje risikotilfælde, herunder om der foreligger en iboende høj risiko for de registrerede. Dokumentationen for valg eller fravalg af konsekvensanalyse noteres i risikovurderingen.

Databehandleraftaler
Systemejeren eller lederen af det pågældende område, som overlader personoplysninger til en ekstern part, har ansvar for at indgå databehandleraftaler for den pågældende behandling eller system, samt opfølgning på, at kravene i databehandleraftalen herunder tilsyn efterleves.

Brug af skabeloner
Jammerbugt Kommune anvender en tilpasset version af Datatilsynets skabelon til databehandleraftaler, og skabelonen kan findes på Tryk.

Det anbefales altid, at kommunens egen skabelon anvendes. Hvis det ikke er muligt at blive enige herom med en databehandler, kræver det et grundigt forarbejde af kommunen, hvor den nye skabelon detaljeret gennemgås for at sikre, at denne lever op til gældende lovgivning. Derudover skal systemejer være opmærksom på, at der i kommunens skabelon som udgangspunkt stilles krav om, at databehandleren på egen regning udleverer en revisionserklæring, som udgør et tilsyn. Ved anvendelse af andre skabeloner kan der derfor være en økonomisk udgift forbundet med tilsynsopgaven, hvis revisionserklæring ikke er noteret som værende vederlagsfrit.

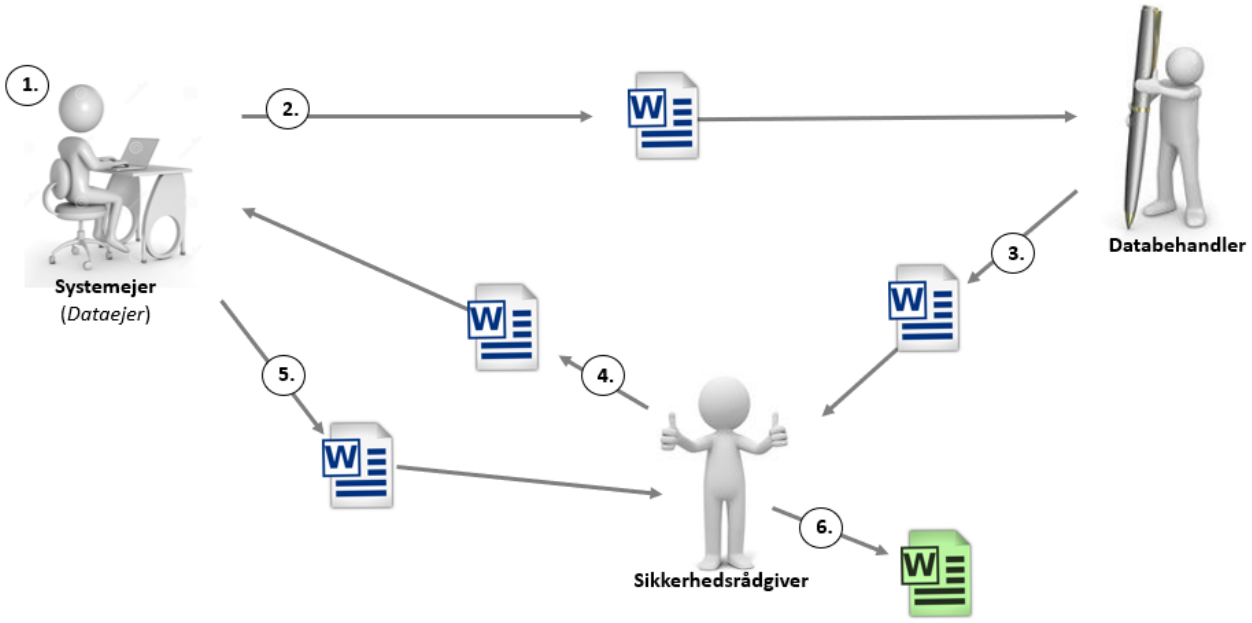
Proces for indgåelse af databehandleraftaler
Det anbefales, at databehandleraftaler indgås, inden hovedkontrakten (fx it-kontrakten) underskrives. Det skyldes, at der kan være økonomiske udgifter forbundet med forpligtelserne i databehandleraftalen (fx tilsyn med databehandleren eller sletning af personoplysninger), og kommunen befinder sig i en dårlig forhandlingsposition med leverandører, når kontrakter om tjenester allerede er indgået. Systemejer bør derfor sikre sig, at der er

enighed om placeringen af de økonomiske udgifter, der er forbundet med de databeskyttelsesretlige forpligtelser, inden en endelig aftale underskrives.

Jammerbugt Kommune indgår i et tværkommunalt samarbejde kaldet Databehandlersekretariatet (DBS), og DBS forhandler udkast til databehandleraftaler på plads med de fleste af kommunens it-leverandører. Jammerbugt Kommune benytter som udgangspunkt DBS' udkast til aftaler. Sikkerhedsrådgiveren sikrer løbende, at kommunen får indgået DBS' aftalerne, når disse foreligger. Det sker ved, at sikkerhedsrådgiveren sender udkastene til systemejeren, som underskriver dokumentet, hvorefter sikkerhedsrådgiveren registrerer og journaliserer aftalen i kommunens systemer.

Når DBS ikke står for forhandlingen af databehandleraftaler på kommunens vegne, foregår processen for indgåelse af databehandleraftaler som følgende:

1. Systemejere finder kommunens skabelon på TRYK og udfylder følgende oplysninger markeret med grønt i skabelonen: Side 1 og 2, afsnit 14.5, 15.2 samt Bilag A1). Hvis det ikke er muligt for systemejeren at udfylde enkelte af de førnævnte oplysninger, beder systemejeren leverandøren om udfyldelse heraf, jf. punktet herunder.
2. Systemejer sender den delvist udfyldte standardskabelon til leverandøren, som udfylder de resterende oplysninger markeret med grønt.
3. Når leverandøren har udfyldt de resterende felter, returneres den til databehandleraftaler@jammerbugt.dk
4. Sikkerhedsrådgiveren kvalitetssikrer aftalen og forhandler evt. aftalevilkår på plads med leverandøren, inden sikkerhedsrådgiveren returnerer den endelige aftale til systemejeren, som nu kan underskrive dokumentet. Hvis der indgår økonomiske vilkår eller prisreguleringer i databehandleraftalen, gør sikkerhedsrådgiveren systemejeren opmærksom herpå, hvorefter systemejeren kan tage stilling til, om kommunen fortsat ønsker at indgå kontrakt med leverandøren.
5. Sikkerhedsrådgiveren journaliserer og registrerer aftalen i systemoversigten og ESDH-systemet.



Figur 1: Proces ved indgåelse af databehandleraftaler

Kontrol af databehandleraftaler

Hvis det er længe siden, at en databehandleraftale blev indgået eller fornyet, kan der være brug for at indgå en ny og opdateret udgave af aftalen. Systemejerne er ansvarlige for at sikre sig, at databehandleraftaler er tilstrækkeligt opdaterede. Dette kan gøres ved at bede sikkerhedsrådgiveren om at tjekke en databehandleraftale igennem, hvis der er gået flere år siden indgåelsen, eller ved at systemejer sammenholder den indgåede databehandleraftale med kommunens standardskabelon, som ligger tilgængeligt på TRYK.

Sikkerhedsrådgiveren kan vejlede i forhold til behovet for indgåelse af en ny databehandleraftale ud fra gældende standarder og vil desuden håndtere den eventuelle videre proces, hvis det vurderes, at aftalen bør genindgås.

Jammerbugt Kommune indgår i et tværkommunalt samarbejde kaldet Databehandlersekretariatet (DBS), hvorfor DBS løbende sikrer, at der indgås opdaterede udkast til databehandleraftaler for de fleste af kommunens leverandører. Sikkerhedsrådgiveren sikrer løbende, at kommunen får indgået DBS' aftalerne, når disse foreligger, jf. afsnittet Proces for indgåelse af databehandleraftaler.

Tredjelandsoverførsler til usikre lande

Enhver overførsel af personoplysninger til usikre tredjelande eller internationale organisationer er betragtet som ulovlig, medmindre leverandøren har et overførselsgrundlag jf. databeskyttelsesforordningen kapitel V.

Jammerbugt Kommune er opmærksomme på problematikken omkring tredjelandsoverførsler som følge af Schrems II-dommen og arbejder gennem forskellige fora, blandt andet i KL-regi, på at forbedre og løse udfordringerne, der findes i de kommunale leverandørers set-up.

Jammerbugt Kommune har desuden til hver en tid et overblik over systemer, som overfører personoplysninger til tredjelande, og prøver at indgå aftaler med leverandørerne om at reducere eller undgå overførslerne. Reducering af overførsler kan bestå af en skriftlig instruks, dataminimering af overførsler, kryptering, pseudonymisering af personoplysninger eller andre relevante metoder.

Derudover vurderer Jammerbugt Kommune altid fremtidige leverandørers tredjelandsoverførsler, og kommunen vil, hvor det er muligt, forhandle yderligere sikkerhedsforanstaltninger vedrørende overførslerne, inden databehandleraftale og kontrakt er underskrevet.

Tilsyn med databehandler og underdatabehandler
Formålet med at føre tilsyn med databehandlere er, at kommunen som dataansvarlig sikrer sig, at de indgåede databehandleraftaler overholdes, herunder at databehandleren gennemfører de aftalte tekniske og organisatoriske sikkerhedsforanstaltninger. Der skal både føres tilsyn med it-leverandører og leverandører af serviceydelser.

Der er ikke faste regler for omfang eller metode for kontrol af databehandlere og underdatabehandlere, men valget af tilsynsformen skal baseres på den risikovurdering, som den dataansvarlige har foretaget:

- Hvis risikoen for de registreredes rettigheder er høj, bør metoden afspejle en hyppig og grundig tilsynsform som fx årlige tilsyn i form af revisionserklæring eller fysisk besøg hos databehandleren og underdatabehandleren.
- Hvis risikoen for de registrerede vurderes lav, kan det være tilstrækkeligt med fx et skriftligt tilsyn hvert andet år.

Sikkerhedsrådgiveren kan rådgive mht. fastlæggelse af tilsynsform og -hyppighed baseret på den konkrete risikovurdering. Det anbefales, at systemejer anvender en systematisk tilgang til opgaven med tilsyn, således der løbende føres tilsyn efter faste bestemmelser på planlagte tidspunkter på året.

Hvordan kan et tilsyn foregå?
Der findes fire muligheder for at føre tilsyn med en databehandler, som alle uddybes i afsnittet herunder:

1. **Revisionserklæring** - Systemejer får databehandleren til at udlevere en revisionserklæring udarbejdet af en ekstern uafhængig tredjepart (f.eks. et revisionsselskab).
2. **Eget skriftligt tilsyn** - Systemejer sender en række kontrolspørgsmål til databehandler og beder denne om skriftligt at besvare spørgsmålene.
3. **Eget fysisk tilsyn** - Systemejer påser behandlingssikkerheden hos sin databehandler og dokumenterer sine observationer i et tilsynsnotat.
4. **Eget tilsyn via ekstern uafhængig tredjepart** – Hvis der er tale om en meget kompleks databehandlersituation eller en situation, hvor der ikke er de rette kompetencer til rådighed, til at føre tilsynet, kan en ekstern tredjepart indkaldes. Dette kan eventuelt anvendes i de konstellationer, hvor flere kommunale eller andre offentlige aktører deler samme databehandler.

Valget af tilsynsform og hyppighed noteres i risikovurderingen.

Revisionserklæring som tilsyn
Systemejer eller systemforvalter bør som minimum ved gennemgang af revisionserklæringer sikre kvaliteten af den modtagne erklæring ved en vurdering af:

- Erklæringens formelle kvalitet: Ser erklæringen legitim ud?
- Erklæringstypen: Hvilken type erklæring er der tale om?
  - Jammerbugt Kommune accepterer revisionserklæring ISAE 3000 og/eller ISAE 3402. Andre typer erklæringer kan ikke udgøre et tilstrækkeligt tilsyn med en databehandler.
- Perioden, som erklæringen gælder for: Som regel vil systemejer ved udlevering af erklæringer ældre end 1 år skulle efterspørge en nyere erklæring.
- Beskrivelsen af databehandlerens ydelse: Forholder erklæringen sig til den konkrete ydelse, databehandleren leverer til kommunen?
- Revisors kompetence: Er der tale om en statsautoriseret revisor?
- Det reelle indhold i erklæringen, det udførte arbejde og konklusioner: Hvad har revisoren kommenteret på, og har revisoren nogle kritikpunkter?
- Eventuelle forbehold og afvigelser: Har revisoren ikke haft mulighed for at undersøge visse elementer til bunds? Evt. kan der være behov for at stille opfølgende spørgsmål til databehandleren for at få svar på de pågældende spørgsmål.
- Komplementerende kontroller/kundens ansvar: Kommunen skal forholde sig til erklæringens eventuelle afsnit om komplementerende kontroller/kundens ansvar. Kommunen skal kunne dokumentere, at man har levet op til de forpligtelser, som noteres som kommunens ansvar.

Giver kvalitetssikringen anledning til opfølgning, bør der afhængig af arten tages en dialog med databehandleren og/eller den erklæringsafgivende revisor.

Til hjælp til ovenstående vurdering findes et skema, som kan bruges til formålet. Denne kan findes på Tryk, og den udfyldte dokumentation skal gemmes på SBSYS-sagen med databehandleraftalen.

Eget tilsyn (skriftligt og fysisk)
Hvis det ikke er muligt eller hensigtsmæssigt at anvende revisionserklæring som tilsynsform, kan systemejeren selv forestå tilsynet – enten ved et skriftligt eller et fysisk tilsyn. Som udgangspunkt vil et skriftligt tilsyn være tilstrækkeligt for langt de fleste databehandlinger, idet databehandleren gennem besvarelse af kontrolspørgsmål kommer bredt omkring de aftalte sikkerhedsforanstaltninger. I *'Bilag 1: Eksempel på kontrolspørgsmål'* kan systemejeren hente hjælp til at gennemføre et skriftligt tilsyn.

Et fysisk tilsyn kan være ressourcekrævende tidsmæssigt, administrativt og økonomisk, blandt andet fordi leverandører ofte vil forlange betaling for en sådan type tilsyn. Fordelen ved at foretage et fysisk besøg vil dog være, at man med egne øjne kan se og fornemme databehandlerens fysiske rammer og arbejdsmetoder. Det bør derfor overvejes, hvorvidt

et fysisk tilsyn kunne være velegnet til databehandlinger af en større mængde følsomme persondata. *'Bilag 1: Eksempler på kontrolspørgsmål'* kan med fordel anvendes som udgangspunkt for kontrollen.

Eget tilsyn via ekstern uafhængig tredjepart
Jammerbugt Kommune indgår i et tværkommunalt samarbejde kaldet Databehandlersekretariatet (DBS), som på vegne af sine medlemskommuner udfører tilsyn med kommunernes databehandlere. I de tilfælde, hvor DBS udfører tilsyn med en af kommunens databehandlere, skal systemejeren sikre sig:

- At der udarbejdes skriftlig dokumentation af, at kommunen har forholdt sig til resultatet af tilsynet og kan tilslutte sig DBS' konklusioner. Dette gøres ved udfyldelse af 'Skabelon til afslutning af tilsyn', som findes på Tryk.
- At kommunen efterlever eventuelle komplementerende kontroller.
- At al relevant dokumentation for tilsynet herunder tilsynsbilag som revisionserklæringer mv. journaliseres i kommunens ESDH-system under databehandleraftale-sagen.

Tilsyn med underdatabehandlere
Kommunen har som dataansvarlig ansvaret for at sikre, at databehandleren fører tilsyn med, at eventuelle underdatabehandlere overholder de databeskyttelsesretlige forpligtelser. Det er således databehandlerens opgave at forestå tilsynene, men kommunen skal kunne dokumentere, at man har bedt om bekræftelse på, at databehandleren har foretaget tilsynene.

Hvis databehandleren benytter sig af godkendte underdatabehandlere, skal kommunen derfor sikre sig, at databehandleren udfører sin opgave med tilsyn fx ved, at databehandleren sender dokumentation for afholdte tilsyn til den dataansvarlige.

Bilag 1: Eksempel på kontrolspørgsmål
Nedenstående skema indeholder kontrolspørgsmål, som samlet set kan udgøre et skriftligt tilsyn med en databehandler.

Det er vigtigt at vurdere, hvorvidt spørgsmålene er relevante for den konkrete databehandler – er der fx andre områder, der er mere relevante at spørge ind til? Skal tilsynet skifte fokus fra gang til gang, således tilsynet nogle gange har særligt fokus på tekniske sikkerhedsforanstaltninger, og andre gange har fokus på interne politikker og procedurer. Du er velkommen til at drøfte kontrolspørgsmålene med sikkerhedsrådgiveren, hvis du ønsker sparring.

Det anbefales, at tilsynsskemaet sendes i en redigerbar version (Word-fil), så databehandleren har mulighed for at besvare spørgsmålene elektronisk.

Kontrolspørgsmålene er baseret på sikringsområderne i ISO 27001 og ISO 27002 samt databeskyttelsesforordningen.

Tilsyn med databehandler				
	Områder	**Kontrolspørgsmål**	**Databehandlerens svar**	**Kommunens vurdering**
A. Behandlingssikkerhed				
A1	Informationssikkerhedspolitik	Findes der en ledelsesgodkendt politik for informationssikkerhed, og er den opdateret indenfor det sidste år? I bedes vedhæfte politikken for informationssikkerhed.		
	Organisering af informationssikkerhed	Er alle roller og ansvarsområder inden for informationssikkerhed defineret og fordelt?		
	Personalesikkerhed	Sikres det løbende, at alle medarbejdere ved hjælp af efteruddannelse og træning bevidstgøres om sikkerhed og regelmæssigt holdes ajour med organisationen politikker og procedurer i det omfang, det er relevant for den enkeltes jobfunktion? I bedes beskrive faste procedurer herfor.		
A2	Styring af aktiver	Er der udarbejdet og implementeret procedurer til håndtering af aktiver i overensstemmelse med det informationsklassifikationssystem, som		

		organisation har vedtaget?		
A3	Kryptografi	Er der udarbejdet og implementeret forskrifter for kryptering af personoplysninger herunder en politik for håndtering af krypteringsnøgler/certifikater?		
	Sletning af data	Er der udarbejdet skriftlige retningslinjer for sletning af data? I bedes vedhæfte pågældende retningslinjer.		
	Hjemmearbejdspladser	Er der etableret hjemmearbejdspladser efter Datatilsynets regler?		
A4	Driftssikkerhed	Er alle driftsprocedurer dokumenteret og gjort tilgængelige for alle de brugere, som har brug for dem?		
A5	Anskaffelse, udvikling og vedligeholdelse af systemer	Er information i forbindelse med applikationstjenester over offentlige netværk beskyttet mod svindel, kontraktlige uoverensstemmelser og uautoriseret offentliggørelse og ændring?		
	Leverandørforhold	Er alle relevante informationssikkerhedskrav fastlagt og aftalt med hver enkelt leverandør, som kan få adgang til, behandle, lagre, kommunikere eller levere IT-infrastrukturkomponenter til organisationen?		
A6	Styring af informationssikkerhed	Er der i forbindelse med sikkerhedsbrud defineret procedurer, som beskriver indsamling, anskaffelse og opbevaring af information, der kan tjene som dokumentation? I bedes beskrive jeres procedure i forbindelse med sikkerhedsbrud.		
	Informationssikkerhedsaspekter ved nød-, beredskabs- og	Er der fastlagt, beskrevet, implementeret og vedligeholdt processer, procedurer og kontroller for at sikre den		

	reetableringsstyring	nødvendige informationssikkerhedskontinuitet i en kritisk situation? (*fx beredskabsplaner*)		
	Overensstemmelse	Ledelsen skal regelmæssigt sikre sig, at informationsbehandlingen og øvrige procedurer i virksomheden, er i overensstemmelse med den relevante sikkerhedspolitikker, standarder og sikkerhedskrav.		
A7	Outsourcet drift	Foreligger der databehandleraftaler med databehandlerens underleverandører?		
	Eksterne leverandører	Er eksterne leverandører, underleverandører og serviceleverandører bekendt med sikkerhedskravene i aftalen med den dataansvarlige?		
	Eksterne konsulenter	Er eksterne konsulenter og lignende bekendt med sikkerhedskravene i aftalen med den dataansvarlige, og foreligger der en underdatabehandleraftale, såfremt der er tale om en databehandlerrelation?		
A8	Adgang til bygning	Foreligger der skriftlige retningslinjer for fysisk sikring? I bedes vedhæfte retningslinjerne.		
	Bygningsforhold	Er der adskillelse mellem offentlige rum og interne kontorlokaler?		
	Sikring af serverum	Er serverrum sikret imod brand, vand og andre hændelser?		
A9	Password	Er der udarbejdet skriftlige retningslinjer for brug af password? I bedes vedhæfte retningslinjerne.		
	Time-out/screensaver	Anvendes der screensaver med lås eller anden timeoutfunktion for at minimere risiko for uautoriseret adgang?		

	Logning	Er der etableret skriftlige retningslinjer for logning på platforme, således at der opnås sporbarhed? I bedes vedhæfte retningslinjerne.		
	Åbne netværk	Er der etableret skriftlige retningslinjer for brug af åbne netværk med henblik på at sikre personoplysninger? I bedes vedhæfte retningslinjerne.		
A10	Brugeradministration	Er der etableret skriftlige retningslinjer for autorisation af brugere med hensyn til adgang til data, som er omfattet af persondataloven? I bedes vedhæfte retningslinjerne.		
	Brugeradministration Certifikater (fortrolige data)	Foreligger der skriftlige retningslinjer, som definerer ansvaret for certifikatoprettelse og -nedlæggelse, og som angiver, hvilke kriterier der oprettes, blokeres og nedlægges efter? I bedes vedhæfte retningslinjerne.		
A11	Krav om arbejdsbehov	Der er kun tildelt dokumenterede adgange i overensstemmelse med arbejdsmæssigt behov.		
	Krav om arbejdsbehov (admin)	Er der udarbejdet særlige skriftlige retningslinjer for personer med administrative privilegier?		
A12	Revurdering af brugerrettigheder	Foretages der periodisk revurdering af brugerrettigheder? I bedes vedhæfte dokumentation på en gennemført kontrol af adgangsrettigheder og resultatet heraf.		
A13	Sikkerhedskopiering	Er der udarbejdet skriftlige retningslinjer for sikkerhedskopiering? I bedes vedhæfte retningslinjerne.		
	Opbevaring af sikkerhedskopiering	Der anvendes sikret opbevaring af backup for at sikre mod uautoriseret adgang.		

	Kryptering af sikkerhedskopi-ering	Der anvendes kryptering af backup indeholdende personoplysninger for at sikre mod uautoriseret adgang.		
A14	Uddatamateriale (makulering mv.)	Er der udarbejdet skrift-lige retningslinjer, der sikrer, at data ikke kom-promitteres i forhold til fortrolighed, herunder sikker bortskaffelse af print mv? I bedes ved-hæfte retningslinjerne.		
A15	Reparationer	Er der udarbejdet skrift-lige retningslinjer for sik-ker bortskaffelse af data og for reparation af ud-styr indeholdende per-sondata? I bedes ved-hæfte retningslinjerne.		
A16	Kommunikati-onslinjer	Er der udarbejdet skrift-lige retningslinjer for eksterne kommunikati-onslinjer for at sikre per-sonoplysninger? I bedes vedhæfte retningslin-jerne.		
A17	Instruktion (be-handling af data)	Medarbejdere er instru-erede i, hvorledes be-handling af data skal ske.		
A18	Overdragelse af data til leveran-dør	Overdragelse af data til leverandører sker sik-kert og ved skriftlig kon-trakt. Ved overdragelse er der udarbejdet kon-trakt og truffet sikrings-foranstaltninger.		
B. Den registreredes rettigheder				
B1	Oplysningspligt	Den dataansvarlige har opfyldt din oplysnings-pligt. Beskriv, hvordan databehandleren evt. hjælper den dataansvar-lige med opfyldelse af oplysningspligten.		
B2	Ret til indsigt, indsigelse, be-rigtigelse og sletning	Er der indført foranstalt-ninger til sikring af den registreredes ret til ind-sigt, indsigelse, berigti-gelse og sletning? Her-under forefindes der skriftlige retningslinjer til sikring af den registrere-des ret til at få indsigt i		

		egne data, at gøre indsigelser mod en behandling, at kræve urigtige oplysninger rettet og at få slettet personoplysninger?		
B3	Samtykke	I tilfælde af, at databehandlingen omfatter brug af samtykke: Er der indført foranstaltninger til sikring af den registreredes ret til at tilbagekalde samtykke? Hvordan håndteres tilbagekaldelser af samtykke hos databehandleren?		
C. Krav til applikationen og det omkringliggende miljø				
C1	Firewall-konfiguration	Er data sikret igennem brug af firewall, der er konfigureret i overensstemmelse med den dataansvarliges sikkerhedspolitik (jf. Sikkerhedsbekendtgørelsen § 14)?		
C2	Virusbeskyttelse	Gør databehandleren brug af antivirus-systemer, som beskytter data, og som opdateres med seneste definitioner?		
C3	Sikkerhedsopgraderinger	Databehandleren gennemfører kontinuerligt sikkerhedsopdateringer af applikationer mv. med henblik på at imødegå "sikkerhedshuller" i applikationer mv.		
C4	Fysisk sikring	Er der på betryggende vis etableret fysisk sikring af platforme? Er der herunder etableret sikring imod brand, vand og andre hændelser i form af eksempelvis nødstrøm, køling og brandslukning?		
C5	Backup	Gennemfører databehandleren backup og sikkerhedskopiering i overensstemmelse med kravene i Sikkerhedsbekendtgørelsen?		

C6	Tekniske platforme	Er den logiske sikkerhed på platformen for applikationen konfigureret korrekt og hensigtsmæssigt i forhold til Sikkerhedsbekendtgørelsen?		
C7	Logning (applikation)	Er der etableret den fornødne logning på applikationsniveau, så alle adgange til- og behandlinger af data logges?		

Med underskriften bekræftes på tro og love korrektheden af oplysningerne.

Dato:_____

_____

Underskrift databehandler