Vejledning til indgåelse af databehandleraftale

Hvorfor skal vi indgå databehandleraftaler?

Når en virksomhed eller en organisation behandler personoplysninger på vegne af Fredensborg Kommune indgår den i rollen som databehandler. En databehandler kan både være en leverandør af et IT-system eller en serviceydelse. Behandlingen af oplysningerne vil altid udføres i Kommunens interesse og ikke i databehandlerens.

Hvis Kommunen overlader behandling af personoplysninger til en databehandler, skal Kommunen sikre sig, at databehandleren har de nødvendige tekniske og organisatoriske sikkerhedsforanstaltninger på plads i sin organisation.

Opgaven, der udføres af databehandleren, skal være reguleret i en databehandleraftale. Aftalen skal beskrive databehandlingsopgaven og parternes roller og ansvar.

Hvornår skal der (ikke) indgås en databehandleraftale?

Der skal indgås en databehandleraftale når hovedformålet er behandling af personoplysninger, og en leverandør varetager en opgave på vegne af og med instruks fra Kommunen (eksempelvis fagsystemer som Acadre og Nexus).

Der skal IKKE indgås en databehandleraftale når:

- Personoplysninger udelukkende behandles (anvendes og lagres) hos os selv
- En aftale først og fremmest drejer sig om en anden ydelse end behandling af personoplysninger (eksempel: håndværkerydelser eller kurser)
- Ved videregivelse til en anden selvstændig dataansvarlig (eksempel: Movia, madudbringning, tøjvask). I nogle tilfælde kan en fortrolighedsaftale være påkrævet
- Der er tale om et system, hvor der udelukkende indtastes ”login-oplysninger” og ikke andre personlysninger (eksempel: Schultz og andre betalbare opslagsydelser)
- Kommunen henter personoplysninger i et system og anvender disse til videre sagsbehandling (eksempel: CPR)
- Videregivelse i forbindelse med visitering (eksempel: Madudbringning)
- Vikar som arbejder hos kommunen.

Hvordan skal en databehandleraftale indgås?

I Fredensborg Kommune anvender vi en skabelon, der er baseret på Datatilsynets udgave. På HosFrede finder du skabelonen med tilhørende vejledning.

FREDENSBORG KOMMUNE

Proces for indgåelse af databehandleraftale:

	Opgave	Hvad	Hvordan
1	Kend data og de registrerede (Borgere, elever, ansatte mv.)	Hvilke typer af data skal leverandøren behandle/ bliver der behandlet i systemet? Hvilke persongrupper behandles der oplysninger om (borgere, børn, patienter, samarbejdspartnere, medarbejdere el.lign.) og ca. hvor mange personer drejer det sig om?	
2	Kend formål, hjemmel og behandlingsaktivitet	Hvorfor bliver der behandlet persondata og i hvilken lov er der en behandlingshjemmel til at gøre det?	
3	Kend leverandør-kæden og dataflowet	Hvor strømmer data hen, bl.a. til andre systemer, andre virksomheder, myndigheder mv., og kan eller bliver der overført data til et land uden for EU/EØS (eksempelvis ifm. support fra leverandøren).	Bed leverandøren om at kortlægge leverandørkæden og dataflowet.
3.1	Overføres der persondata til et tredjeland = et land uden for EU/EØS? (Tilsigtet overførsel)	Overfører leverandøren data til en underdatabehandler eller en anden del af organisationen beliggende i et tredjeland: • Er der indgået et gyldigt overførselsgrundlag? • Er der udarbejdet en Transfer Impact Assesment (TIA) af leverandøren? • Hvilke supplerende foranstaltninger er implementeret for at sikre, at borgernes rettigheder i det væsentligste svarer til det de har inden for EU? • Lav en skriftlig vurdering af leverandørens TIA. Ligger leverandøren i et tredjeland, så Kommunen overfører data direkte til et tredjeland: • Udarbejd en Transfer Impact Assesment (TIA). • Hvilke supplerende foranstaltninger skal implementeres for at sikre, at borgernes rettigheder i det væsentligste svarer til det de har inden for EU?	Spørg leverandøren. Benyt 'Skabelon-TIA' til både vurdering af leverandørs TIA eller egen TIA. Liste over godkendte tredjelande, der kan overføres persondata til: https://www.datatilsynet.dk/internationalt/tredjelandsoverfoersler

3.2	Særligt om USA	Er der tale om en amerikansk leverandør eller underdatabehandler, kan der overføres personoplysninger til leverandøren, hvis organisationen er certificeret efter EU-U.S Data Privacy Framework. Er organisationen ikke certificerede, skal overførslen behandles som en tredjelandsoverførsel som under punkt 3.1.	Find listen med certificerede organisationer: https://www.dataprivacyframework.gov/s/participant-search
4	Bruger leverandøren oplysningerne til sit eget formål?	Det kan eksempelvis være serviceoplysninger til at forbedre systemet. Videregives data til leverandørens egen brug, skal der være en udtrykkelig hjemmel til at vi kan videregive persondata til leverandøren.	Spørg leverandøren, læs i betingelser mv.
5	Risikovurdering(er)	Kommunen skal, før en behandling foretages, lave en kortlægning over risikoen for de registreredes rettigheder og en afvejning af disse risici i forhold til de forholdsregler der bliver truffet for at beskytte disse rettigheder. Dokumentationen skal afspejle overvejelser og valg (og fravalg)	Laves i Wired Relations.
6	Evt. konsekvensanalyse (DPIA)	Hvis risikovurderingen viser at behandlingen medfører en høj risiko for borgerne skal der udarbejdes en konsekvensanalyse. Det gælder ligeledes, hvis der bl.a. er tale om: - Ny teknologi - Stor mængde af personoplysninger eller oplysninger om en stor mængde af personer - Der behandles oplysninger om sårbare fysiske personer, f.eks. børn eller psykisk syge.	'Skabelon – Konsekvensanalyse'
7	Valg af tilsynskoncept	Når Kommunen bruger en databehandler, er vi ansvarlige for, at databehandleren behandler personoplysningerne efter den instruks der er givet i databehandleraftalen. Det sikrer vi bl.a. ved, at føre tilsyn med databehandlerens overholdelse af databehandleraftalen. Det er derfor vigtigt, at det er aftalt i databehandleraftalen, hvordan og hvor ofte der skal føres tilsyn. Et tilsyn kan som udgangspunkt foregå på 2 måder: • Databehandleren laver en egenerklæring, som tilsynet tager udgangspunkt i.	Benyt 'Skabelon – valg af tilsynskoncept', til at fastlægge tilsynskoncept.

		• Databehandleren får udarbejdet en revisorerklæring som tilsynet tager udgangspunkt i.	
8	Indgå databehandleraftale	Der er to typer af skabeloner: • Hvor al databehandling foregår inden for EU/EØS: Skabelon baseret på Datatilsynets standardbestemmelser. • Hvor databehandleren er beliggende uden for EU/EØS: Skabelon til 'Standard Kontrakt Bestemmelser (SCC). Henvend dig til GDPR-teamet.	Skabelon med vejledning findes på HosFrede.
9	Sammenfatning og dokumentation	Al ovenstående materiale og vurderinger skal gemmes sammen med databehandleraftalen i Wired Relations.	
10	Opsætning og test af systemet inden ibrugtagning	Systemet skal sættes korrekt op fra start, med de rigtige indstillinger, brugerrettigheder og andet. Der skal laves test af systemet, så det sikres, at det er sat korrekt og sikkert op. Der skal laves en procedure for oprettelse og nedlæggelse af brugeradgange, samt laves en procedure for kontrol med brugeradgange.	