Vejledning og tjekliste til indgåelse af databehandleraftaler

En virksomhed, som er arbejdsgiver, er "dataansvarlig", når virksomheden behandler personoplysninger som led i personaleadministrationen. Virksomheden bestemmer f.eks., hvilke personoplysninger vedrørende en jobansøgers uddannelsesbaggrund, der er nødvendige for at vurdere kandidatens egnethed. Som dataansvarlig er virksomheden direkte ansvarlig for behandlingen af personoplysninger over for jobansøgere samt nuværende og tidligere ansatte.

I forbindelse med personaleadministration og øvrige arbejdsgiveropgaver, kan virksomheden indgå forskellige aftaler med databehandlere om ekstern bistand. Der er f.eks. tale om databehandlere, når en cloudleverandør (f.eks. online hosting) opbevarer personoplysninger for en virksomhed; når et servicebureau varetager lønudbetalingen til virksomhedens ansatte.

Når en virksomhed antager en databehandler til at behandle personoplysninger på virksomhedens vegne, er det et krav, at den dataansvarlige (lægepraksis) og databehandleren (leverandøren eller samarbejdspartneren) indgår en skriftlig databehandleraftale.

Bruun & Hjejle har i samarbejde med Praktiserende Lægers Arbejdsgiverforening (PLA) udarbejdet skemaet i bilag 1, som er en kort vejledning, som kan hjælpe virksomheden med at finde ud af, hvornår tredjeparter er selvstændigt dataansvarlige eller er databehandlere, som forudsætter indgåelse af en skriftlig databehandleraftale.

Herudover har Bruun & Hjejle i samarbejde med PLA også udarbejdet en oversigt i bilag 2 over, hvilke forhold der som minimum skal reguleres. Oversigten er udformet, så den kan anvendes som tjekliste i forbindelse med udarbejdelse eller gennemgang af aftaleudkast modtaget fra en samarbejdspartner.

Bilag 1

Vejledning: Dataansvarlig vs. databehandler		
Dataansvarlig		**Databehandler**
Den/de dataansvarlige **definerer formålene med og hjælpemidlerne til behandling af personoplysninger.**		Databehandleren **behandler personoplysninger på vegne af den dataansvarlige.**
Vejledning		**Vejledning**
Den dataansvarlige afgør: ■ Om personoplysninger skal behandles. ■ Hvilke personoplysninger, der skal behandles. ■ På hvilket retsgrundlag behandlingen baseres. ■ Formålet/-ene med behandlingen. ■ Hvilke personer personoplysningerne omhandler. ■ Hvem, der skal modtage personoplysningerne. ■ Om anmodninger om udnyttelse af den registreredes rettigheder imødekommes og i hvilket omfang. ■ I hvor lang tid personoplysningerne behandles (dvs. hvornår de slettes). ■ Hvilke tredjeparter, der må få adgang til personoplysningerne.		En databehandler kan få beføjelse til at afgøre følgende på vegne af den dataansvarlige: ■ Hvilke IT-systemer eller –metoder, der anvendes i forbindelse med behandling af personoplysninger. ■ Hvordan og hvilket sted, personoplysninger opbevares, f.eks. servernes beliggenhed. ■ Hvilke tekniske og organisatoriske sikkerhedsforanstaltninger, der skal implementeres. ■ Hvordan personoplysninger indsamles. ■ Hvordan personoplysninger videregives til tredjeparter. ■ Hvilke procedurer, der gennemføres for at sikre, at personoplysninger slettes inden for slettefristerne. ■ Hvordan underdatabehandlere auditeres (forudsat tilstrækkelighed).
Eksempler – her skal I <u>ikke</u> bruge en databehandleraftale: ■ Rekrutteringsfirma, som rekrutterer specialister til en virksomhed. ■ SKAT. ■ Eksterne leverandører af revision og juridisk bistand. ■ Pensionsselskaber. ■ Forsikringsselskab, som tilbyder forsikringsdækning til en virksomheds ansatte. ■ En læge, som udfærdiger en medicinsk rapport i forbindelse med en forsikringssag. (I disse tilfælde får den dataansvarlige overdraget oplysninger, men anvender dem til **egen forretning** og **uden instruks)**		**Eksempler – her <u>skal</u> I bruge en databehandleraftale:** ■ Systemhusene. ■ Softwareudbyder, som leverer forretningsløsninger, f.eks. et HR-administrationssystem, og som sørger for driften af systemet. ■ Ekstern lønadministration, f.eks. Bluegarden, Danløn mv. ■ Udbyder af møde- eller aftalebookingsystem (med hosting af dataene). ■ Udbyder af e-mail-marketing services. ■ Hosting-udbyder, herunder cloud-udbydere. ■ Leverandør af medarbejdertilfredshedsundersøgelser. (I disse tilfælde får databehandleren overdraget oplysninger og anvender dem **på vegne af** lægeklinikken og **efter instruks**)
Ovenfor er anført en række typiske eksempler på rollen som henholdsvis dataansvarlig og databehandler. Vær opmærksom på, at eksemplerne kun er vejledende. Det vil derfor være nødvendigt at foretage en egentlig juridisk vurdering af den dataansvarliges eller databehandlerens rolle, hvis fordelingen af ansvar mellem parterne ikke er i overensstemmelse med ovenstående vejledende principper.		

Bilag 2

Tjekliste til databehandleraftaler

Bruun & Hjejle har i marts 2018 udarbejdet denne tjekliste til PLA til brug for gennemgang af databehandleraftaler fra tredjeparter. Tjeklistens pkt. 1 indeholder et overblik over, hvilke klausuler, der er obligatoriske at have med i en databehandleraftale men udgør ikke de endelige formuleringer til databehandleraftalen. Derudover er der indsat ikke-udtømmende eksempler på frivillige klausuler i tjeklistens pkt. 2. Tjeklisten udgør ikke juridisk rådgivning.

Kontraktens parter _____

Kontraktnavn _____

Dato: _____

Medarbejdernavn: _____

1. Obligatoriske klausuler

Reference	Generelle krav	Kontrakt pkt./bilag
Art. 28 (3)	Reguleret af en bindende kontrakt. Aftalen skal fastsætte • genstanden for behandlingen	
	• varigheden af behandlingen	
	• behandlingens karakter og formål	
	• typen af personoplysninger	
	• kategorierne af registrerede	
	• den dataansvarliges forpligtelser og rettigheder (som udmøntes i de følgende afsnit)	
Reference	**Instrukser**	
Art. 28(3)(a) + 32(4)	Databehandleren og enhver person, der arbejder på vegne af databehandleren, må kun behandle personoplysninger efter dokumenterede instrukser fra den dataansvarlige, herunder også overførsel af personoplysninger til et tredjeland eller en international organisation, medmindre det kræves i henhold til EU-ret eller medlemsstaternes nationale ret, som databehandleren er underlagt; i så fald underretter databehandleren den dataansvarlige om dette retlige krav inden behandling, medmindre den pågældende ret forbyder en sådan underretning af hensyn til vigtige samfundsmæssige interesser.	

Art. 28(3)(b)	Personer, der er bemyndiget til at behandle personoplysninger, skal forpligte sig til fortrolighed enten kontraktuelt eller via passende lovbestemt tavshedspligt.	
Art. 28(3)(h)	Databehandleren skal omgående underrette den dataansvarlige, hvis en instruks efter databehandlerens mening er i strid med forordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret.	
Reference	**Sikkerhed**	
Art. 28(3)(c) + art. 32	Databehandleren skal implementere passende tekniske og organisatoriske foranstaltninger for at beskytte Personoplysningerne. *Kommunikation af personoplysninger skal ske over sikre forbindelser. Personoplysninger, der overføres eller opbevares uden for et lukket netværk kontrolleret af Databehandleren, skal beskyttes med kryptering. Hvor det er passende og hensigtsmæssigt henset til oplysningernes karakter, skal oplysningerne desuden pseudonomiseres.* *Adgangskontroller og –begrænsninger skal indføres i passende omfang. Fysisk materiale, der indeholder personoplysninger, opbevares aflåst.* *Databehandleren skal sørge for løbende sikkerhedskopiering af personoplysningerne. Kopierne skal opbevares adskilt og forsvarligt og på en måde som sikrer mulighed for at oplysningerne kan genskabes.* *Databehandleren har som led i databehandleraftalen forpligtet sig til én gang årligt at afgive en erklæring til den dataansvarlige, der dokumenterer, at databehandleraftalen handler i overensstemmelse med gældende persondataret. Erklæringen baseres på ISAE 3402 eller tilsvarende. Erklæringen skal være underskrevet af en kvalificeret, uvildig instans, f.eks. databehandlerens revisor.*	
Reference	**Underdatabehandlere**	
Art. 28(3)(d) Jf. stk. 2	Enten generel bemyndigelse til brug af underdatabehandlere med indsigelsesret for den dataansvarlige eller krav om specifik tilladelse fra dataansvarlige. Ved generel godkendelse, skal databehandleren underrette den dataansvarlige om eventuelle planlagte ændringer vedrørende tilføjelse eller erstatning af andre databehandlere og derved give dataansvarlige mulighed for at gøre indsigelse.	
Art. 28(3)(d) Jf. stk. 4	Det er en forudsætning for antagelse af en underdatabehandler, at Databehandleren indgår en skriftlig aftale med underdatabehandleren om, at underdatabehandleren pålægges de samme databeskyttelsesforpligtelser og kontraktuelle betingelser, som dem der er fastsat i aftalen mellem den Dataansvarlige og Databehandleren. Hvis underdatabehandleren ikke overholder sine forpligtelser forbliver databehandleren fuldt ansvarlig over for den dataansvarlige for opfyldelsen af den underdatabehandlerens forpligtelser.	
Reference	**Bistandsforpligtelser**	
Art. 28(3)(f)	Databehandleren skal bistå med at sikre overholdelse af forpligtelserne i medfør af artikel 32-36 under hensyntagen til behandlingens karakter og de oplysninger, der er tilgængelige for databehandleren.	

Art. 28(3)(e)	Databehandleren skal bistå den dataansvarlige, ved hjælp af passende tekniske og organisatoriske foranstaltninger, med opfyldelse af den dataansvarliges forpligtelser til at besvare anmodninger om udøvelse af de registreredes rettigheder: - Ret til at få indsigt - Ret til berigtigelse - Ret til sletning - Ret til begrænsning af behandling - Ret til dataportabilitet - Ret til indsigelse	
Reference	**Påvisning af overholdelse, revisioner**	
Art. 28(3)(h)	Databehandleren stiller alle de oplysninger til rådighed for den dataansvarlige, der er nødvendige for at påvise overholdelse af lovgivningsmæssige krav.	
Art. 28(3)(h)	Databehandleren skal give mulighed for og bidrage til revisioner, herunder inspektioner, der foretages af den dataansvarlige eller en anden revisor, som er bemyndiget af den dataansvarlige.	
Reference	**Varighed og ophør**	
Art. 28(3)(g)	Databehandleren skal efter den dataansvarliges valg slette eller tilbagelevere alle personoplysninger til den dataansvarlige, når serviceydelserne vedrørende behandling er ophørt, medmindre ufravigelig lovgivning foreskriver opbevaring af personoplysningerne.	

2. Eksempler på bestemmelser, som ikke er et krav efter forordningens regler og som er til fordel for databehandleren (og derfor ikke bør accepteres af jer uden forudgående, individuel rådgivning)

Information om lovgivning
Kommentar: Jeres leverandører bør selv sørge for at holde sig opdateret om gældende ret. Ofte kender de reglerne bedre end jer, særligt de tekniske krav. Nedenfor ses et eksempel på en bestemmelse herom, som ikke uden videre bør accepteres: Den dataansvarlige skal informere databehandleren om enhver national lovgivning, der ud over persondatalovgivningen kan være relevant for behandlingen eller opbevaringen af personoplysninger.
Betaling for revisioner osv.
Kommentar: Nogle leverandører vil forsøge at opnå særskilt betaling for erklæring om/revision af at deres håndtering af jeres data foregår lovligt og i overensstemmelse med gældende sikkerhedskrav. Nedenfor ses et eksempel på en bestemmelse herom, som ikke uden videre bør accepteres: Assistance fra databehandleren og eventuelle underdatabehandlere til revisioner, inspektioner osv. Skal udføres på baggrund af en aftale om omfang, metode og pris.
Honorar til databehandleren
Kommentar: Nogle databehandlere vil opstille krav om særskilt honorar for at stille den dokumentation til rådighed, som de er forpligtede til at levere ifølge forordningens regler, herunder f.eks. i forbindelse med et sikkerhedsbrud. Nedenfor ses et eksempel på en bestemmelse herom, som ikke uden videre bør accepteres: Den dataansvarlige skal betale databehandleren honorar for tid medgået til opfyldelse af en række af kontraktens bestemmelser, f.eks. bestemmelser om årlig dokumentation for sikkerhed, bistand til sikkerhedsbrist, håndtering af sletning osv.
Erstatningsansvar
Kommentar: Nogle databehandlere vil forsøge at medtage bestemmelser, som begrænser deres erstatningsansvar over for jer. Det skal ikke uden videre accepteres. Bestemmelsen kan formuleres på mange måder men kan f.eks. se ud som bestemmelserne nedenfor. Databehandleren er alene erstatningsansvarlig for skade eller tab over for den dataansvarlige, enten ved direkte krav eller regreskrav, såfremt skaden eller tabet skyldes ansvarspådragende fejl eller forsømmelser fra databehandlerens side. Hver parts erstatningsansvar kan ikke overstige [XX] kr.
Regres for erstatningsansvar
Kommentar: Nogle databehandlere vil forsøge at medtage bestemmelser om, at hvis de bliver pålagt at betale erstatning, kan de søge beløbet tilbage hos jer, dvs. at I skal "skadeløsholde" databehandleren. Dette bør I ikke acceptere uden forudgående, individuel rådgivning.