Tjekliste til databehandleraftaler

Bruun & Hjejle har i november 2017 udarbejdet denne tjekliste til brug for gennemgang af databehandleraftaler modtaget fra samarbejdspartnere. Tjeklistens pkt. 1 indeholder et overblik over, hvilke klausuler, det er obligatorisk at have med i en databehandleraftale men ikke de endelige formuleringer til databehandleraftalen. Derudover er der indsat ikke-udtømmende eksempler på frivillige klausuler i tjeklistens pkt. 2.

Tjeklisten er udarbejdet så den omfatter de generelle krav, der opstilles i databeskyttelsesforordningen i forhold til indgåelse af databehandleraftaler. Det betyder samtidig, at der i konkrete samarbejder kan være behov for at regulere flere forhold, end dem, der fremgår af tjeklisten. Er du i tvivl, bør du søge individuel, juridisk rådgivning inden kontaktindgåelsen.

1. Obligatoriske bestemmelser

Reference	Generelle krav	Kontrakt pkt./bilag
Art. 28 (3)	**Aftalen skal fastsætte:** • **genstanden** for behandlingen *(dvs. hvad er det, systemet eller den eksterne leverandør skal hjælpe med, fx opbevaring af journaloplysninger, udarbejdelse af analyser eller statistikker osv.)*	
	• **varigheden** af behandlingen *(dvs. hvor længe, den systemethuset eller den eksterne part forventes at skulle bistå. Det kan fx være et bestemt antal måneder eller år, eller det kan være "indtil videre", "indtil aftalen opsiges" osv.)*	
	• behandlingens **karakter** og **formål** ***(****dvs. hvad det er, systemhuset eller den eksterne part skal hjælpe med, fx indsamlingen, registrering, opbevaring, anonymisering, sammenstilling, formidling til kvalitetsdatabaser osv.)*	

	• **typen af personoplysninger** *(fx stamdata, herunder cpr-nr., helbredsoplysninger, oplysninger om behandlingsforløb osv.)*	
	• **kategorierne af registrerede** *(fx patienter i praksis)*	
	• den dataansvarliges forpligtelser og rettigheder (se de følgende afsnit, som skal fremgå udtrykkeligt af databehandleraftalen)	
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.** Dette gælder enhver form for behandling, som databehandleren foretager på vegne af den dataansvarlige. **Databehandleren kan dog behandle oplysninger uden dokumenterede instrukser fra den dataansvarlige,** hvis behandlingen er påkrævet efter EU-retlige regler eller medlemsstaternes nationale regler, som databehandleren er underlagt. Hvis databehandleren er forpligtet efter EU- eller nationale regler skal **databehandleren underrette den dataansvarlige om disse regler, inden behandlingen påbegyndes,** medmindre de pågældende regler forbyder en sådan underretning af hensyn til vigtige samfundsmæssige interesser (fx efterforskningssager).	
Art. 28(3)(b)	Personer, der er bemyndiget til at behandle personoplysninger, **skal forpligte sig til fortrolighed enten i en kontrakt eller via passende lovbestemt tavshedspligt**.	
Art. 28(3)(h)	Databehandleren skal forpligtes til omgående at 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)	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 kontrolleren 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 mig (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 af brugen af underdatabehandlere, skal databehandleren underrette den dataansvarlige om eventuelle planlagte udskiftninger eller udvidelse i kredsen af underdatabehandlere og 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 kontraktlige betingelser, som dem der er fastsat i aftalen mellem den dataansvarlige og databehandleren. Hvis underdatabehandleren ikke overholder sine forpligtelser, er 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 vedrørende i medfør af artikel 32-36** (regler om behandlingssikkerhed) under hensyntagen til behandlingens karakter og de oplysninger, der er tilgængelige for databehandleren.	
Art. 28(3)(e)	Databehandleren skal **bistå den dataansvarlige, så vidt muligt med passende tekniske og organisatoriske foranstaltninger, med opfyldelse af den dataansvarliges forpligtelser til at besvare anmodninger** om udøvelse af de registreredes rettigheder: Indsigt, berigtigelse, sletning, begrænsning af behandling, dataportabilitet, indsigelse.	
Reference	**Påvisning af overholdelse, revisioner**	
Art. 28(3)(h)	Databehandleren skal **stille alle de oplysninger til rå-**	

	dighed 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 systemhuse eller andre eksterne 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 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 systemhuse eller andre eksterne 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: Bidrag fra databehandleren og eventuelle underdatabehandlere til revisioner, inspektioner osv. underlægges 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 fx 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, fx 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 fx 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 [XXX] x 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.