



## Databehandlersaftale

Mellem

Den dataansvarlige:

Selskabets navn:	Dansk Dermatologisk Selskab
CVR-nummer:	DK19643573
Adresse:	c/o CAP, Nordre Fasanvej113, 2.
Postnummer og by:	2000 Frederiksberg

og

Databehandleren:

Lægeforeningen  
CVR-nummer: 12067313  
Kristianiagade 12  
2100 København Ø





## 1 Baggrund for databehandleraftalen

1. Denne aftale fastsætter de rettigheder og forpligtelser, som finder anvendelse, når databehandleren foretager behandling af personoplysninger på vegne af den dataansvarlige.
2. Aftalen er udformet med henblik på parternes efterlevelse af artikel 28, stk. 3, i **Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (Databeskyttelsesforordningen)**, som stiller specifikke krav til indholdet af en databehandleraftale.
3. Databehandlerens behandling af personoplysninger sker med henblik på at leve op til selskabets og Lægeforeningens aftale om bistand til selskabet.
4. Denne databehandleraftale har forrang i forhold til eventuelle tilsvarende bestemmelser i andre aftaler mellem parterne.
5. Aftalens bilag er en integreret del af databehandleraftalen.
6. Databehandleraftalens Bilag A indeholder nærmere oplysninger om behandlingen, herunder om behandlingens formål og karakter, typen af personoplysninger, kategorierne af registrerede og varighed af behandlingen.
7. Databehandleraftalens Bilag B vedrører databehandlerens brug af underdatabehandlere.
8. Databehandleraftalens Bilag C indeholder en nærmere instruks om, hvilken behandling databehandleren skal foretage på vegne af den dataansvarlige (behandlingens genstand), hvilke sikkerhedsforanstaltninger, der som minimum skal iagttages, samt hvordan der kan føres tilsyn med databehandleren.
9. Databehandleraftalen med tilhørende bilag opbevares skriftligt, herunder elektronisk af begge parter.
10. Denne databehandleraftale frigør ikke databehandleren for forpligtelser, som efter databeskyttelsesforordningen eller enhver anden lovgivning direkte er pålagt databehandleren.

## 2 Den dataansvarliges forpligtelser og rettigheder

1. Den dataansvarlige har overfor omverdenen (herunder den registrerede) som udgangspunkt ansvaret for, at behandlingen af personoplysninger sker indenfor rammerne af databeskyttelsesforordningen og databeskyttelsesloven.
2. Den dataansvarlige har derfor både rettighederne og forpligtelserne til at træffe beslutninger om, til hvilke formål og med hvilke hjælpemidler der må foretages behandling.
3. Den dataansvarlige er blandt andet ansvarlig for, at der foreligger hjemmel til den behandling, som databehandleren instrueres i at foretage.

## 3 Databehandleren handler efter instruks

1. Databehandleren må kun behandle personoplysninger efter dokumenteret instruks, jf. bilag C, fra den dataansvarlige, 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, jf. art 28, stk. 3, litra a.



2. Databehandleren underretter omgående den dataansvarlige, hvis en instruks efter databehandlerens mening er i strid med databeskyttelsesforordningen eller databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret.

#### 4 Fortrolighed

1. Databehandleren sikrer, at kun de personer, der aktuelt er autoriseret hertil, har adgang til de personoplysninger, der behandles på vegne af den dataansvarlige. Adgangen til oplysningerne skal derfor straks lukkes ned, hvis autorisationen fratages eller udløber.

På grund af databehandlerens organisering har alle databehandlerens medarbejdere adgang til oplysninger om medlemskab af dataansvarliges organisation. Disse oplysninger tilgås og anvendes imidlertid kun, når det er relevant for opgaveløsningen i relation til den dataansvarlige.

2. Databehandleren sikrer, at de personer, der er autoriseret til at behandle personoplysninger på vegne af den dataansvarlige, har forpligtet sig til fortrolighed.
3. Databehandleren skal efter anmodning fra den dataansvarlige kunne påvise, at de relevante medarbejdere er underlagt ovennævnte tavshedspligt.

#### 5 Behandlingssikkerhed

1. Databehandleren iværksætter alle foranstaltninger, som kræves i henhold til databeskyttelsesforordningens artikel 32, hvoraf det bl.a. fremgår, at der under hensyntagen til det aktuelle niveau, implementeringsomkostningerne og den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder skal gennemføres passende tekniske og organisatoriske foranstaltninger for at sikre et sikkerhedsniveau, der passer til disse risici.
2. Ovenstående forpligtelse indebærer, at databehandleren skal foretage en risikovurdering, og herefter gennemføre foranstaltninger for at imødegå identificerede risici. Der kan herunder bl.a., alt efter hvad der er relevant, være tale om følgende foranstaltninger:
  - a. Pseudonymisering og kryptering af personoplysninger
  - b. Evne til at sikre vedvarende fortrolighed, integritet, tilgængelighed og robusthed af behandlingssystemer og -tjenester
  - c. Evne til rettidigt at genoprette tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse
  - d. En procedure for regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske foranstaltninger til sikring af behandlingssikkerhed
3. Databehandleren skal i forbindelse med ovenstående - i alle tilfælde - som minimum iværksætte det sikkerhedsniveau og de foranstaltninger, som er specificeret nærmere i denne aftales Bilag C.

#### 6 Anvendelse af underdatabehandlere

1. Databehandleren skal opfylde de betingelser, der er omhandlet i databeskyttelsesforordningens artikel 28, stk. 2 og 4, for at gøre brug af en anden databehandler (underdatabehandler), se tillige Bilag B.



2. Hvis underdatabehandleren ikke opfylder sine databeskyttelsesforpligtelser, forbliver databehandleren fuldt ansvarlig over for den dataansvarlige for opfyldelsen af underdatabehandlerens forpligtelser.

## 7 Overførsel af oplysninger til tredjelande eller internationale organisationer

1. Databehandleren må kun behandle personoplysninger efter dokumenteret instruks fra den dataansvarlige, herunder for så vidt angår overførsel (overladelse, videregivelse samt intern anvendelse) af personoplysninger til tredjelande eller internationale organisationer, 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, jf. art 28, stk. 3, litra a.

## 8 Bistand til den dataansvarlige

1. Databehandleren bistår, under hensyntagen til behandlingens karakter, så vidt muligt den dataansvarlige ved hjælp af passende tekniske og organisatoriske foranstaltninger, med opfyldelse af den dataansvarliges forpligtelse til at besvare anmodninger om udøvelsen af de registreredes rettigheder som fastlagt i databeskyttelsesforordningens kapitel 3.

Dette indebærer, at databehandleren så vidt muligt skal bistå den dataansvarlige i forbindelse med, at den dataansvarlige skal sikre overholdelsen af:

- a. oplysningspligten ved indsamling af personoplysninger hos den registrerede
  - b. oplysningspligten, hvis personoplysninger ikke er indsamlet hos den registrerede
  - c. den registreredes indsigtret
  - d. retten til berigtigelse
  - e. retten til sletning (»retten til at blive glemt«)
  - f. retten til begrænsning af behandling
  - g. underretningspligt i forbindelse med berigtigelse eller sletning af personoplysninger eller begrænsning af behandling
  - h. retten til dataportabilitet
  - i. retten til indsigelse
  - j. retten til at gøre indsigelse mod resultatet af automatiske individuelle afgørelser, herunder profilering
2. Databehandleren bistår den dataansvarlige med at sikre overholdelse af den dataansvarliges forpligtelser i medfør af databeskyttelsesforordningens artikel 32-36 under hensyntagen til behandlingens karakter og de oplysninger, der er tilgængelige for databehandleren, jf. art 28, stk. 3, litra f.

Dette indebærer, at databehandleren under hensyntagen til behandlingens karakter skal bistå den dataansvarlige i forbindelse med, at den dataansvarlige skal sikre overholdelsen af:

- a. forpligtelsen til at gennemføre passende tekniske og organisatoriske foranstaltninger for at sikre et sikkerhedsniveau, der passer til de risici, der er forbundet med behandlingen
- b. forpligtelsen til at anmelde brud på persondatasikkerheden til tilsynsmyndigheden (Datatilsynet) uden unødigt forsinkelse og om muligt senest 72 timer, efter at den dataansvarlige er blevet bekendt med bruddet, medmindre at det er usandsynligt, at bruddet på persondatasikkerheden indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder.



- c. forpligtelsen til - uden unødigt forsinkelse - at underrette den/de registrerede om brud på persondatasikkerheden, når et sådant brud sandsynligvis vil indebære en høj risiko for fysiske personers rettigheder og frihedsrettigheder
  - d. forpligtelsen til at gennemføre en konsekvensanalyse vedrørende databeskyttelse, hvis en type behandling sandsynligvis vil indebære en høj risiko for fysiske personers rettigheder og frihedsrettigheder
  - e. forpligtelsen til at høre tilsynsmyndigheden (Datatilsynet) inden behandling, såfremt en konsekvensanalyse vedrørende databeskyttelse viser, at behandlingen vil føre til høj risiko i mangel af foranstaltninger truffet af den dataansvarlige for at begrænse risikoen.
3. Bistanden efter dette pkt. 9 er ikke forudsat i parternes bestående aftaleforhold, hvorfor parterne er enige om, at der ikke på tidspunktet for databehandleraftalens indgåelse er taget endelig stilling til spørgsmålet om vederlag for denne bistand.

## 9 Underretning om brud på persondatasikkerheden

1. Databehandleren underretter uden unødigt forsinkelse den dataansvarlige efter at være blevet opmærksom på, at der er sket brud på persondatasikkerheden hos databehandleren eller en eventuel underdatabehandler.

Databehandlerens underretning til den dataansvarlige skal ske snarest efter at denne er blevet bekendt med bruddet, sådan at den dataansvarlige har mulighed for at efterleve sin eventuelle forpligtelse til at anmelde bruddet til tilsynsmyndigheden indenfor 72 timer.

2. I overensstemmelse med denne aftales afsnit 10.2, litra b, skal databehandleren - under hensyntagen til behandlingens karakter og de oplysninger, der er tilgængelige for denne - bistå den dataansvarlige med at foretage anmeldelse af bruddet til tilsynsmyndigheden.

Det kan betyde, at databehandleren bl.a. skal hjælpe med at tilvejebringe nedenstående oplysninger, som efter databeskyttelsesforordningens artikel 33, stk. 3, skal fremgå af den dataansvarliges anmeldelse til tilsynsmyndigheden:

- a. Karakteren af bruddet på persondatasikkerheden, herunder, hvis det er muligt, kategorierne og det omtrentlige antal berørte registrerede samt kategorierne og det omtrentlige antal berørte registreringer af personoplysninger
- b. Sandsynlige konsekvenser af bruddet på persondatasikkerheden
- c. Foranstaltninger, som er truffet eller foreslås truffet for at håndtere bruddet på persondatasikkerheden, herunder hvis det er relevant, foranstaltninger for at begrænse dets mulige skadevirkninger

## 10 Sletning og tilbagelevering af oplysninger

1. Ved ophør af tjenesterne vedrørende behandling forpligtes databehandleren til, efter den dataansvarliges valg, at slette eller tilbagelevere alle personoplysninger til den dataansvarlige, samt at slette eksisterende kopier, medmindre EU-retten eller national ret foreskriver opbevaring af personoplysningerne.

## 11 Tilsyn og revision

1. Databehandleren stiller alle oplysninger, der er nødvendige for at påvise databehandlerens overholdelse af databeskyttelsesforordningens artikel 28 og denne aftale, til rådighed for den dataansvarlige og giver mulighed for og bidrager til revisioner, herunder inspektioner, der foretages af den dataansvarlige eller en anden revisor, som er bemyndiget af den dataansvarlige.



## 12 Ikrafttræden og ophør

1. Denne aftale træder i kraft ved begge parter underskrift heraf.
2. Aftalen kan af begge parter kræves genforhandlet, hvis lovændringer eller uhensigtsmæssigheder i aftalen giver anledning hertil.
3. Opsigelse af databehandleraftalen kan ske i henhold til de opsigelsesvilkår, inkl. opsigelsesvarsel, som fremgår af parternes øvrige aftale.
4. Databehandleraftalen forbliver i kraft frem til behandlingens ophør og oplysningernes sletning hos databehandleren og eventuelle underdatabehandlere.
5. Underskrift

På vegne af den dataansvarlige

På vegne af databehandleren

Navn: Christina Skovbølling Haak

Navn: Bente Hyldahl Fogh

Stilling: Webmaster, DDS

Stilling: Adm. direktør

Dato: 22. oktober 2019

Dato: 19. september 2019

Underskrift:

Underskrift:



## Bilag A      Oplysninger om behandlingen

### **Formålet med databehandlerens behandling af personoplysninger på vegne af den dataansvarlige er:**

- at databehandleren kan behandle oplysninger om den dataansvarliges medlemmer i forbindelse med kontingentopkrævning, afholdelse af og indkaldelse til kurser, vedligeholdelse af hjemmeside, øvrig sekretariatsbistand, herunder indkaldelse til bestyrelsesmøder og andre møder i den dataansvarliges organisation.

### **Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige drejer sig primært om (karakteren af behandlingen):**

- at databehandleren ved anvendelse af sine IT-systemer behandler, herunder opbevarer, personoplysninger om den dataansvarliges medlemmer.

### **Behandlingen omfatter følgende typer af personoplysninger om de registrerede:**

- Navn, e-mailadresse, telefonnummer, adresse, cpr-nummer, foto, betalingsoplysninger, medlemsnummer, type af medlemskab, stillingsbetegnelse.

Da denne databehandleraftale, jf. pkt. 1.3-4 skal ses i sammenhæng med parternes grundlæggende aftale, vil den konkrete bistand til selskabet fremgå af denne grundlæggende aftale, hvorved typen af behandlede personoplysninger kan variere alt efter den tilkøbte bistand hos databehandleren.

### **Behandlingen omfatter følgende kategorier af registrerede:**

- Personer, som har eller har haft et medlemskab hos den dataansvarlige.

### **Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige kan påbegyndes efter denne aftales ikrafttræden. Behandlingen har følgende varighed:**

- Behandlingen er ikke tidsbegrænset og varer indtil aftalen opsiges eller ophæves af en af parterne.

### **Kontaktpersoner/kontaktpunkter hos den dataansvarlige og databehandleren:**

1. Parterne kan kontakte hinanden ved de for det hidtidige samarbejde sædvanlige kontaktpersoner/kontaktpunkter.
2. Parterne er forpligtet til løbende at orientere hinanden om ændringer vedrørende kontaktpersoner/kontaktpunktet.



## Bilag B      Betingelser for databehandlerens brug af underdatabehandlere

### A.1 Betingelser for databehandlerens brug af eventuelle underdatabehandlere:

Databehandleren har den dataansvarliges generelle godkendelse til at gøre brug af underdatabehandlere. Databehandleren fører på den dataansvarliges vegne tilsyn og kontrol med underdatabehandlerne.

På anmodning kan den dataansvarlige på ethvert tidspunkt få udleveret en fuldkommen liste over databehandlerens brug af underdatabehandlere. Denne fremsendes uden ugrundet ophold.

Måtte den dataansvarlige have indvendinger mod brugen af en eller flere underdatabehandlere, vil dette i udgangspunktet medføre, at databehandleren bringer det samlede aftaleforhold til ophør, medmindre den dataansvarlige har rimelige, konkrete årsager til sin indvending mod en eller flere underdatabehandlere.





## Bilag C Instruks vedrørende behandling af personoplysninger

### Generelt

Databehandleren skal i forbindelse med behandling af personoplysningerne som minimum træffe de nødvendige tekniske og organisatoriske sikkerhedsforanstaltninger, jf. aftalens pkt. 5.

Herudover skal databehandleren træffe de nedenfor beskrevne tekniske og organisatoriske sikkerhedsforanstaltninger i forbindelse med behandling af personoplysningerne;

#### 1. Operationel sikkerhed

1.1 Databehandleren skal sikre;

- (A) at det nødvendige sikkerhedsniveau vedligeholdes og opretholdes, samt at eventuelle ændringer i databehandlerens sikkerhedsforanstaltninger relevante for personoplysningerne logges og dokumenteres,
- (B) at ændringer og vedligeholdelse af databehandlerens sikkerhedsforanstaltninger så vidt muligt ikke påvirker den dataansvarliges forretning, herunder men ikke begrænset til it-systemer, netværk, forbindelser og svartider. Ved mulig påvirkning skal den dataansvarlige orienteres inden iværksættelse af tiltag.
- (C) at alle komponenter i databehandlerens eller underdatabehandlerens IT-ydelser, herunder, men ikke begrænset til IT-systemer (alle miljøer), servere og netværk, er tilstrækkeligt sikret mod hacking mv. og anden uautoriseret adgang,
- (D) at databehandleren gennemfører, og kan dokumentere, tilstrækkelig overvågning og kontrol i henhold til god IT-skik og eventuelle branchestandarder, for at opdage og forhindre svindel, malware mv., og
- (E) at dennes interne operationelle sikkerhedsprocedurer følges.

#### 2. Fysisk sikkerhed

2.1 Databehandleren skal sikre sine fysiske lokaliteter, servere mv. mod uautoriseret adgang.

2.2 Databehandleren skal have interne sikkerhedsprocedurer der ved fjernelse, afhændelse eller genbrug af hardware sikrer, at den dataansvarliges personoplysninger ikke kompromitteres.

#### 3. Backup

3.1 Databehandleren skal foretage backup af personoplysninger mv. samt teknisk test af backup.

3.2 Backup'en skal være krypteret.

#### 4. Adgang til Personoplysninger

4.1 Databehandleren skal sikre, at kun relevante medarbejdere har adgang til de behandlede Personoplysninger.



- 4.2 Databehandleren skal efter den dataansvarliges anmodning på ethvert tidspunkt kunne afgive en erklæring om hvilke personer, som har haft adgang til personoplysningerne på vegne af databehandleren.
- 4.3 Databehandleren skal sikre, at enhver person, der udfører arbejde for databehandleren og får adgang til personoplysningerne, kun behandler sådanne oplysninger efter den dataansvarliges instruks, medmindre behandlingen er påkrævet i henhold til EU-lovgivningen eller EØS-medlemsstaternes nationale lovgivning.
- 4.4 Databehandleren skal sikre, at enhver person, der udfører arbejde for databehandleren og får adgang til personoplysningerne har oparbejdet tilstrækkeligt kendskab til korrekt håndtering af personoplysninger, og at de pågældende medarbejdere er bekendt med de for aftalen gældende sikkerhedskrav.
- 4.5 Databehandler skal informere dataansvarlig om ethvert fjendtligt forsøg på at få adgang til personoplysninger, herunder eksempelvis hacking og uautoriseret adgang.

## **5. Logning**

- 5.1 Databehandler foretager logning i overensstemmelse med lovgivningen og gældende branchestandarder.
- 5.2 Der skal foretages logning af alle afviste adgangsforsøg. Hvis der inden for en periode på 24 timer er registreret højst 5 (fem) på hinanden følgende afviste adgangsforsøg fra samme bruger, skal der blokeres for yderligere forsøg. Adgangen må først åbnes, når årsagen er klarlagt og dokumenteret.
- 5.3 Der skal foretages maskinel logning af alle anvendelser af personoplysninger. Loggen skal mindst indeholde oplysninger om tidspunkt, bruger, type af anvendelse og angivelse af den person, de anvendte oplysninger vedrører eller det anvendte søgekriterium.
- 5.4 Den dataansvarlige kan på anmodning få de relevante logs udleveret fra Databehandleren.
- 5.5 Log opbevares i 6 måneder.

## **6. Nærmere procedurer for den dataansvarliges tilsyn med den behandling, som foretages hos databehandleren**

- 6.1 Den dataansvarlige eller en repræsentant for den dataansvarlige er berettiget til at foretager fysisk tilsyn vedrørende overholdelsen af denne databehandleraftale hos databehandleren.
- 6.2 Den dataansvarliges eventuelle udgifter i forbindelse med et fysisk tilsyn afholdes af den dataansvarlige selv. Databehandleren er dog forpligtet til at afsætte de ressourcer (hovedsageligt den tid), der er nødvendig for, at den dataansvarlige kan gennemføre sit tilsyn.