Databehandleraftale

Mellem

Den dataansvarlige:

Navn

CVR nummer

Adresse

Postnummer og by

og

Databehandleren

CompuGroup Medical Danmark A/S

CVR-nr. 24210529

Sommervej 31 E, 3. sal

8210 Aarhus V

1 Indhold

2 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 levering af serviceydelser i form af et it-system til brug for behandling af patientoplysninger i den dataansvarliges klinik samt kommunikation og datatransmission til nødvendige tekniske sundhedstjenester via legale transportører og til legale modtagere.

4. Databehandleraftalen og "hovedaftalen" er indbyrdes afhængige, og kan ikke opsiges særskilt. Databehandleraftalen kan dog – uden at opsige "hovedaftalen" – erstattes af en anden gyldig databehandleraftale.

5. Denne databehandleraftale har forrang i forhold til eventuelle tilsvarende bestemmelser i andre aftaler mellem parterne, herunder i "hovedaftalen" såfremt den pågældende uoverensstemmelse omhandler et forhold vedrørende behandling af personoplysninger. Aftalen dækker alene ydelser der er omfattet af Hovedaftalen

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 indeholder den dataansvarliges betingelser for, at databehandleren kan gøre brug af eventuelle underdatabehandlere, samt en liste over de eventuelle underdatabehandlere, som den dataansvarlige har godkendt.

8. Databehandleraftalens Bilag B 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 føres tilsyn med databehandleren og eventuelle underdatabehandlere.

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.

3 Den dataansvarliges forpligtelser og rettigheder

1. Den dataansvarlige har over for omverdenen (herunder den registrerede) som udgangspunkt ansvaret for, at behandlingen af personoplysninger sker inden for 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.

4 Databehandleren handler efter instruks

1. Databehandleren må kun behandle personoplysninger efter dokumenteret instruks 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.

5 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.

2. Der må alene autoriseres personer, for hvem det er nødvendigt at have adgang til personoplysningerne for at kunne opfylde databehandlerens forpligtelser overfor den dataansvarlige.

3. Databehandleren sikrer, at de personer, der er autoriseret til at behandle personoplysninger på vegne af den dataansvarlige, har forpligtet sig til fortrolighed eller er underlagt en passende lovbestemt tavshedspligt.

4. Databehandleren skal efter anmodning fra den dataansvarlige kunne påvise, at de relevante medarbejdere er underlagt ovennævnte tavshedspligt.

6 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.

7 Anvendelse af underdatabehandlere

1. Databehandleren må gøre brug af en anden databehandler (underdatabehandlere) uden forudgående specifik godkendelse fra den Dataansvarlige, forudsat at Databehandleren skriftligt senest 14 dage forinden det planlagte opstartstidspunkt underretter den Dataansvarlige om identiteten på den potentielle underdatabehandler inden indgåelse af aftale med den pågældende underdatabehandler, hvorved den Dataansvarlige får 14 dage for at gøre indsigelse mod ændringer eller tilføjelser. Den Dataansvarliges indsigelse skal indeholde tungtvejende saglige grunde mod anvendelse af den påtænkte underdatabehandler, for at Databehandleren forpligtiges til at efterkomme indsigelsen.

2. Den dataansvarliges har ved denne aftales indgåelse godkendt underdatabehandleren/underdatabehandlerne anført i Bilag B.

3. Databehandleren er således ansvarlig for – igennem indgåelsen af en underdatabehandleraftale – at pålægge en eventuel underdatabehandler mindst de forpligtelser, som databehandleren selv er underlagt efter databeskyttelsesreglerne og denne databehandleraftale med tilhørende bilag.

4. **Hvis underdatabehandleren ikke opfylder sine databeskyttelsesforpligtelser, er databehandleren ansvarlig over for den dataansvarlige på samme måde som for Databehandlerens egne handlinger og undladelser.**

8 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.**

2. Uden den dataansvarliges instruks eller godkendelse kan databehandleren – indenfor rammerne af databehandleraftalen - derfor bl.a. ikke;

    a. videregive personoplysningerne til en dataansvarlig i et tredjeland eller i en international organisation,
    b. overlade behandlingen af personoplysninger til en underdatabehandler i et tredjeland,
    c. lade oplysningerne behandle i en anden af databehandlerens afdelinger, som er placeret i et tredjeland.

3. Den dataansvarliges eventuelle instruks eller godkendelse af, at der foretages overførsel af personoplysninger til et tredjeland, vil fremgå af denne aftales Bilag C.

9 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 indsigtsret
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 hensynstagen til behandlingens karakter og de oplysninger, der er tilgængelige for databehandleren, jf. art 28, stk. 3, litra f.**

Dette indebærer, at databehandleren under hensynstagen 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 unødig 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 unødig 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

10 Honorar til databehandlere

1. Databehandleren har krav på betaling efter medgået tid samt Databehandlerens øvrige omkostninger herved, for de ydelser der udføres efter Databehandleraftalen på den Dataansvarliges anmodning. Ydelserne kan omfatte, men er ikke begrænset til, assistance til den Dataansvarliges forpligtelser efter artikel 32 – 36, ændringer i Aftalen eller instruks, udlevering af oplysninger, bistand ved audit, bistand til Databeskyttelsesforordningens kapitel 3, bistand til ændringer der følger af nye risikovurderinger og konsekvensanalyser, så længe dette ikke beror på manglende levering af aftalte funktioner i de tekniske løsninger, der skal leveres af databehandleren. Dette gælder blandt andet:

   1. Bistand til udlæsning, gennemgang og udredning af log i forbindelse med patientklagesager.

   2. Bistand til kryptering eller anden yderligere sikring af databaser, netværk, servere og andet udstyr der ikke er indeholdt i den Dataansvarliges kontrakt(er) med Databehandleren.

   3. Bistand, ved anmodning fra den Dataansvarlige, til sletning af journaldata, såfremt den Dataansvarlige selv har teknisk tilgængelig mulighed for at kunne foretage sletningen.

2. For ydelser der ikke er omfattet af punkt 9.1 er Databehandleren dog ikke berettiget til vederlag i det omfang Databehandleren jf. lovgivningen er den direkte forpligtede part. Dette gælder kun for ydelser der ydes i relation til services og ydelser omfattet af hovedaftalen

3. Vederlaget opgøres efter de aftalte timesatser i aftale(r)n(e) om levering af Serviceydelserne, og hvor der ikke er aftalt timesatser heri, da efter Leverandørens gældende timesatser, der dog ikke må overskride branchekutyme.

4. Databehandleren har uanset ovenstående ikke krav på betaling for assistance eller implementering af ændringer i det omfang, sådan assistance eller ændring er en direkte følge af Databehandlerens egen misligholdelse af denne Aftale.

11 Underretning om brud på persondatasikkerheden

5. Databehandleren underretter uden unødig 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 om muligt ske senest 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.

6. I overensstemmelse med denne aftales skal databehandleren - under hensynstagen 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

12 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.**

13 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.**

2. Den dataansvarliges tilsyn med eventuelle underdatabehandlere sker som udgangspunkt gennem databehandleren.

3. Databehandleren er forpligtet til at give myndigheder, der efter den til enhver tid gældende lovgivning har adgang til den dataansvarliges og databehandlerens faciliteter, eller repræsentanter, der optræder på myndighedens vegne, adgang til databehandlerens fysiske faciliteter mod behørig legitimation.

14 Parternes aftaler om andre forhold

1. En eventuel (særlig) regulering af konsekvenserne af parternes misligholdelse af databehandleraftalen vil fremgår af parternes "hovedaftale".

2. En eventuel regulering af andre forhold mellem parterne vil fremgå af parternes "hovedaftale".

15 Ikrafttræden og ophør

1. Denne aftale træder i kraft ved begge parters underskrift heraf.

2. Aftalen kan af begge parter kræves genforhandlet, hvis lovændringer eller uhensigtsmæssigheder i aftalen giver anledning hertil.

3. Parternes eventuelle regulering/aftale om vederlæggelse, betingelser eller lignende i forbindelse med ændringer af denne aftale.

3. Opsigelse af databehandleraftalen kan ske i henhold til de opsigelsesvilkår, inkl. opsigelsesvarsel, som fremgår af "hovedaftalen".

4. Aftalen er gældende, så længe behandlingen består. Uanset "hovedaftalens" og/eller databehandleraftalens opsigelse, vil databehandleraftalen forblive i kraft frem til behandlingens ophør og oplysningernes sletning hos databehandleren og eventuelle underdatabehandlere.

5. Underskrift

På vegne af dataansvarlig:	På vegne af databehandler:	
Navn:	Navn:	Michael Hein
Stilling:	Stilling:	Administrerende direktør
Dato:	Dato:	14. maj 2018
Underskrift:	Underskrift:	

Bilag A Oplysninger om databehandlingen

Version 1: 8. maj. 2018

1. Registrerede

Databehandleren behandler personoplysninger om følgende kategorier af registrerede ("Registrerede") på vegne af den Dataansvarlige og følgende type af personoplysninger (herefter benævnt " Personoplysninger") om de Registrerede på vegne af den Dataansvarlige.

	Patienter
Særlige kategorier af personoplysninger	Helbredsoplysninger, race eller etnisk oprindelse seksuelle forhold eller seksuel orientering politisk-, religiøs-, filosofisk overbevisning fagforeningsmæssigt tilhørsforhold oplysninger om straf eller lovovertrædelser samt genetiske eller biometriske oplysninger
Generelle kategorier af personoplysninger	Navn, telefonnummer, postadresse, fødselsdato, mailadresse, cpr.nr, familieforhold, sociale problemer, bolig, stilling, køn

2. Formål

2.1 Databehandlerens behandling af Personoplysninger for den Dataansvarlige sker til følgende formål:
Levering af de aftalte it-ydelser, herunder levering af journalsystem samt kommunikation og datatransmission til nødvendige tekniske sundhedstjenester via legale transportører og til legale modtagere.

3. Databehandlingsaktiviteter/databehandlingens karakter

3.1 Databehandlerens behandling af Personoplysninger for den Dataansvarlige sker i overensstemmelse med hovedaftalen om omfatter bl.a., herunder men ikke begrænset til følgende aktiviteter:

- Ved at opbevare Personoplysninger og sikre systemers tilgængelighed, integritet og fortrolighed
- Ved at yde remote service til den Dataansvarliges brugere af journal- og booking- og økonomisystemerne
- Ved at formidle Personoplysninger til tredjeparter efter den Dataansvarliges instruks
- Sletning

4. Modtagere

4.1 Databehandleren må ud over eventuelle underdatabehandlere videregive Personoplysninger til modtagere, som den Dataansvarlige er forpligtet til at videregive personoplysninger til. Den Dataansvarlige er ansvarlig for, at overholde den til enhver tid gældende

persondatalovgivning i forhold til de personoplysninger, som overlades til Databehandlerens behandling med henblik på videregivelse.

4.2 Den Dataansvarlige er forpligtet til at vedligeholde en liste over disse modtagere.

5. Liste over godkendte underdatabehandlere

Den dataansvarlige har ved databehandleraftalens ikrafttræden godkendt anvendelsen af følgende underdatabehandlere:

Navn	CVR-nr	Adresse	Beskrivelse af behandling
TrueCommerce Danmark	33776349	Banevænget 13 3460 Birkerød	Kommunikation til og fra klinikken til andre parter i sundhedsvæsenet. Herunder men ikke begrænset til henvisninger, epikriser, korrespondancebreve
TDC	14773908	Teglholmsgade 1 2450 Kbh SV	Levering af sikre kommunikationslinjer mellem klinikken og CGM til brug for transport af kommunikation
ipnordic	3357 7591	Nygade 17 6300 Gråsten	IP-telefoni mellem klinik og patienter
Dandomain	25476255	Normannsvej 1 8920 Randers NV	Levering af web-hosting, email-hosting samt fjernbackup
Medcom	26919991	Forskerparken 10 5230 Odense M	Leverandør af sundhedsdatanettet. Et krypteret netværk. Herunder men ikke begrænset til FMK, DDV.

Den dataansvarlige har ved databehandleraftalens ikrafttræden specifikt godkendt anvendelsen af ovennævnte underdatabehandlere til netop den behandling, som er beskrevet ud for parten. Databehandleren kan ikke – uden den dataansvarliges specifikke og skriftlige godkendelse – anvende den enkelte underdatabehandler til en "anden" behandling and aftalt eller lade en anden underdatabehandler foretage den beskrevne behandling.

Bilag B Sikkerhedsinstruks

Databehandleren skal i forbindelse med behandling af Personoplysningerne som minimum træffe de nødvendige tekniske og organisatoriske sikkerhedsforanstaltninger, jf. Aftalens pkt. 6.. Herudover skal databehandleren træffe de nedenfor beskrevne tekniske og organisatoriske sikkerhedsforanstaltninger i forbindelse med behandling af Personoplysningerne;

1. Standarder

1.1 Databehandleren skal efterleve principperne i ISO 27001 på relevante områder eller en i øvrigt anerkendt standard inden for IT-drift, i det omfang andet ikke fremgår af nærværende databehandleraftale.

2. Operationel sikkerhed

2.1 Databehandleren skal sikre;

(A) at det nødvendige og tilstrækkelige 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,

(C) at Databehandlerens eventuelle testmiljøer er tilstrækkelig afgrænset og i øvrigt sikret mod uautoriseret adgang,

(D) at Databehandlerens it-systemer og netværk er tilstrækkeligt sikret mod hacking og anden uautoriseret adgang,

(E) at Databehandleren gennemfører kontroller for at opdage og forhindre svindel, malware mv., og

(F) at dennes interne operationelle sikkerhedsprocedurer og -manualer følges.

3. Fysisk sikkerhed

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

3.2 Databehandleren skal have interne sikkerhedsprocedurer der ved fjernelse, afhændelse eller genbrug af hardware sikrer, at den Dataansvarliges Personoplysninger ikke kompromitteres.

4. Backup

4.1 Databehandleren skal foretage backup af Personoplysningerne samt teknisk test af backup, i det omfang backup er en del af hovedaftalen

4.2 Såfremt det er en del af hovedaftalen, vil Databehandleren herefter én gang i døgnet tage en backup af den Dataansvarliges oplysninger i journalsystemet. Backup-overførslen skal være krypteret. Backup skal opbevares i et aflåst område i en anden bygning end hvor

produktionsserveren fysisk er placeret. Backup gemmes i henhold til den i hovedaftalen definerede periode.

4.3 Databehandleren stiller en erklæring om backup og teknisk test af backup til rådighed for den Dataansvarlige.

5. Adgang til Personoplysninger

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

5.2 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.

5.3 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.

5.4 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.

6. Logning

6.1 Databehandler foretager logning i overensstemmelse med lovgivningen og gældende branchestandarder.

6.2 Der skal foretages logning af alle afviste adgangsforsøg. Hvis der inden for en periode på 24 timer er registreret højst 5 på hinanden følgende afviste adgangsforsøg fra samme bruger, skal der blokeres for yderligere forsøg. Adgangen må først åbnes, når årsagen er klarlagt og dokumenteret.

6.3 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.

6.4 Den Dataansvarlige kan på anmodning få de relevante logs udleveret fra Databehandleren.

6.5 Log opbevares i 6 måneder.

7. Samarbejde med myndigheder

7.1 Databehandleren samarbejder efter anmodning med Datatilsynet og eventuelle øvrige tilsynsmyndigheder i forbindelse med udførelsen af sådanne tilsynsmyndigheders opgaver.

Databehandleren er herunder berettiget til at give Datatilsynet adgang til alle person oplysninger og oplysninger, der er nødvendige for at varetage Datatilsynets opgaver.

Efter Databehandlerens valg træffer enten den Dataansvarlige eller Databehandleren de nødvendige foranstaltninger til at sikre overholdelse af en afgørelse fra Datatilsynet. Eventuelle ændringer i forhold til sikkerhedsniveau gennemføres som en ændring i henhold til denne Aftale. Den Dataansvarlige underretter Datatilsynet om de foranstaltninger, der er truffet for at overholde afgørelsen.

Meddeler Datatilsynet Databehandleren påbud, skal Databehandleren efterkomme sådant påbud i overensstemmelse med den nærmere angivne måde og inden for den angivne frist.

8. Databehandlere, der har adgang til den Dataansvarliges IT-systemer og/eller den Dataansvarlige fysiske bygninger mv.

8.1 Databehandlere, der har adgang til den Dataansvarliges IT-systemer og/eller fysiske bygninger, skal ud over sikkerhedskravene i dette underbilag B, endvidere overholde de af dette punkt 5 omfattede sikkerhedskrav.

8.2 Databehandleren har tilladelse til at tilgå den Dataansvarliges netværk og IT-systemer i det omfang det er nødvendigt i henhold til hovedaftalen. Dette sker via legale og sikkerhedsgodkendte værktøjer og kanaler, jf bilag B.