Journalnummer:

regionernes sundheds-it

DATABEHANDLERAFTALE

Vedrørende Databehandlerens behandling af personoplysninger med henblik på opfyldelse af parternes aftale af xx.xx.201x omhandlende xxxx (herefter "Hovedaftalen")

Mellem

Region

Adresse

Afdeling

CVR-nr.:]

(herefter den *"Dataansvarlige"*)

System-/projektansvarlig person
Tel. +45 XXXX XXXX
e-mail@e-mail.dk

og

Firmanavn

Adresse

Evt. underafdeling

Kontaktperson

CVR-nr.

(herefter *"Databehandleren"*)

Indholdsfortegnelse

1. Baggrund for Databehandleraftalen

1.1. Denne databehandleraftale inklusiv bilag og eventuelle tillæg (herefter "Databehandleraftalen") vedrører Databehandlerens forpligtelse til at efterleve 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 (herefter "Databeskyttelsesforordningen") samt lov om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (herefter "Databeskyttelsesloven").

1.2. Databehandleraftalen er en integreret del af Hovedaftalen.

1.3. I tilfælde af uoverensstemmelser mellem bestemmelserne i Databehandleraftalen og eventuelle tilsvarende bestemmelser i andre aftaler mellem den Dataansvarlige og Databehandleren, herunder i Hovedaftalen, skal bestemmelserne i Databehandleraftalen have forrang. Dette gælder uanset, hvad der i øvrigt måtte være aftalt om forrang. Såfremt Databehandleren er pålagt strengere forpligtelser i andre aftaler mellem den Dataansvarlige og Databehandleren, herunder i Hovedaftalen, skal Databehandleren dog fortsat opfylde disse.

2. Databehandlerens ansvar

2.1. Databehandleren må kun behandle personoplysninger efter dokumenteret instruks fra den Dataansvarlige og alene i det omfang, det er nødvendigt for, at Databehandleren kan opfylde sine forpligtelser i henhold til Hovedaftalen og Databehandleraftalen, 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. Databeskyttelsesforordningens artikel 28, stk. 3, litra a.

Databehandleraftalen er en del af den Dataansvarliges instruks til Databehandleren. Databehandleren behandler personoplysningerne på vegne af den Dataansvarlige, og må ikke behandle personoplysninger omfattet af Databehandleraftalen til egne formål.

2.2. Hvis Databehandleren er undergivet lovgivningen i et tredjeland, skal Databehandleren straks skriftligt orientere den Dataansvarlige, hvis den nævnte lovgivning forhindrer Databehandleren i at efterleve Databehandleraftalen og den dertilhørende instruks.

2.3. Databehandler underretter omgående den Dataansvarlige, hvis en instruks efter Databehandlerens vurdering er i strid med Databeskyttelsesforordningen, Databeskyttelsesloven eller databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret (herefter samlet benævnt "Databeskyttelseslovgivningen")

2.4. Databehandleraftalen frigør ikke Databehandleren for forpligtelser, som efter Databeskyttelsesforordningen, eller den til enhver tid anden gældende lovgivning, direkte er pålagt Databehandleren.

3. Databehandlerens opgave

3.1. Databehandlerens behandling af personoplysninger sker med henblik på opfyldelse af Hovedaftalen.

3.2. Formålet med Databehandlerens behandling er INDSÆT

3.3. Databehandleren opgave er at ...(f.eks. hoste/supportere/drifte systemet etc.) - klar beskrivelse af den databehandling, Databehandleren foretager, herunder hvordan personoplysninger mellem den Dataansvarlige og Databehandleren udveksles.

3.4. Databehandleren behandler følgende typer af personoplysninger:

f.eks. navn, adresse, cpr-nummer, sundhedsdata (diagnose, behandling e.l.), osv. Oplistningen skal så vidt muligt være udtømmende.

3.5. Databehandleren behandler personoplysninger vedrørende følgende kategorier af registrerede:

f.eks. medarbejdere ansat på afdeling XX, patienter med diagnose XX, pårørende til patienter, testpersoner mv., samt (hvis relevant) inklusions- og udvælgelseskriterier.

3.6. De personoplysninger, som er omfattet af Databehandleraftalen, behandles (f.eks. opbevares, hostes, foretages back-up) på følgende adresse(r), herunder også ad hoc arbejdspladser:

INDSÆT

4. Tekniske og organisatoriske sikkerhedsforanstaltninger

4.1. Databehandleren iværksætter alle foranstaltninger, som kræves i henhold til Databeskyttelsesforordningens artikel 32, hvoraf det bl.a. fremgår, at der under hensyntagen til det aktuelle tekniske 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.

4.2. Af bilag 1 (Databehandlerinstruks) fremgår minimumskrav til de fornødne tekniske og organisatoriske sikkerhedsforanstaltninger.

4.3. Principperne og anbefalingerne i ISO 27001, med senere ændringer, vil skulle anvendes som vejledende ramme ved overholdelse af kravene i Databehandleraftalen.

5. Databehandlerens brug af underdatabehandler

5.1. Databehandleren må ikke gøre brug af en anden databehandler (underdatabehandler) til behandling af personoplysninger omfattet af Databehandleraftalen uden den Dataansvarliges forudgående skriftlig godkendelse. Databehandleraftalens bilag 2 angiver de underdatabehandlere, der er godkendt af den Dataansvarlige.

5.2. Databehandleren skal orientere den Dataansvarlige og indhente en specifik godkendelse fra den Dataansvarlige i tilfælde af, at der vælges ny underdatabehandler. Orienteringen skal ske senest 3 måneder inden den nye underdatabehandler tages i anvendelse. Orienteringen skal ske via revidering af bilag 2 og sendes til indsæt kontaktperson.

5.3. Endvidere er Databehandleren forpligtet til, efter anmodning fra den Dataansvarlige at udlevere en systematiseret oversigt over den samlede kæde af underdatabehandlere angivet i bilag 2, hvoraf det tydeligt fremgår, hvordan underdatabehandlerne er indbyrdes relateret.

5.4. Databehandleren skal indgå aftale med underdatabehandleren, hvor underdatabehandleren som minimum forpligtes til at opfylde de databeskyttelsesforpligtelser, som Databehandleren har påtaget sig ved Databehandleraftalen. Underdatabehandleren skal som minimum have samme sikkerhedsniveau, som Databehandleren har påtaget sig med Databehandleraftalen.

5.5. Anvendes en underdatabehandler skal Databehandleren udlevere den indgåede databehandleraftale mellem Databehandleren og underdatabehandleren på forespørgsel fra den Dataansvarlige. Databehandleren skal kunne dokumentere, at underdatabehandleren er blevet instrueret om de sikkerhedskrav, der fremgår af bilag 1 (Databehandlerinstruks).

5.6. Databehandleren er ansvarlig for kontraktmæssigheden og lovligheden af underdatabehandlerens behandling af personoplysninger. Det forhold, at Databehandler indgår aftale med en underdatabehandler, fritager ikke Databehandleren for pligten til at efterleve Databehandleraftalen.

5.7. Ved ophør af en aftale med en underdatabehandler om behandling af personoplysninger omfattet af Databehandleraftalen, skal Databehandleren give den Dataansvarlige meddelelse herom. Databehandleren skal i den forbindelse sikre, at underdatabehandleren sletter personoplysningerne behørigt i overensstemmelse med punkt 10.

5.8. Databehandleren skal i sin aftale med underdatabehandleren for så vidt muligt indføje den Dataansvarlige som begunstiget tredjemand i tilfælde af Databehandlerens konkurs, således at den Dataansvarlige kan indtræde i Databehandlerens rettigheder og gøre dem gældende over for underdatabehandleren for så vidt angår behandling af personoplysninger, f.eks. så den Dataansvarlige kan instruere underdatabehandleren om at foretage sletning eller tilbagelevering af personoplysninger.

6. Overførsel af personoplysninger til tredjelande eller internationale organisationer

6.1. I henhold til Databeskyttelsesforordningen kapitel 5 skal Databehandleren sikre, at der ikke behandles personoplysninger uden skriftlig dokumenteret instruks fra den Dataansvarlige, herunder for så vidt angår overførsel (f.eks. overladelse, videregivelse samt intern anvendelse) af personoplysninger til tredjelande eller internationale organisationer, medmindre Databehandleren er underlagt andre krav i henhold til EU-ret eller medlemsstaternes nationale ret. I så fald underretter Databehandleren den Dataansvarlige om dette retlige krav inden behandlingen, medmindre den pågældende ret forbyder en sådan underretning af hensyn til vigtige samfundsmæssige interesser, jf. Databeskyttelsesforordningens artikel 28, stk. 3, litra a.

6.2. Uden den Dataansvarliges dokumenterede instruks eller skriftlige godkendelse kan Databehandleren derfor blandt andet ikke:

i. Videregive personoplysningerne til en Dataansvarlig i et tredjeland eller i en international organisation.
ii. Overlade behandlingen af personoplysningerne til en underdatabehandler i et tredjeland eller i en international organisation.
iii. Lade personoplysningerne behandle i en anden af Databehandlerens afdelinger, som er placeret i et tredjeland.

6.3. Såfremt den Dataansvarlige har givet Databehandleren en skriftlig godkendelse til overførsel af personoplysninger til en underdatabehandler i et tredjeland, påhviler det Databehandleren at sikre, at personoplysningerne ikke overføres, førend der foreligger et lovligt grundlag for overførsel af personoplysningerne til de pågældende lande. Anvendes en underdatabehandler i et tredjeland, skal dette fremgå i Databehandleraftalens bilag 2.

7. Tilsyn og revision

7.1. Databehandleren stiller alle oplysninger, der er nødvendige for at påvise Databehandlerens overholdelse af Databeskyttelseslovgivningen og Databehandleraftalen, 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.

7.2. Der er i Databehandleraftalen aftalt følgende tilsyn INDSÆT

7.3. 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. Databehandleren forpligter sig på samme måde til at sikre, at sådanne inspektioner også kan gennemføres hos dennes eventuelle underdatabehandlere.

7.4. Databehandleren er forpligtet til at føre tilsyn med eventuelle underdatabehandlere. Databehandlerens tilsyn med underdatabehandlere skal følge den aftalte procedure for

tilsyn. Databehandleren skal efter anmodning dokumentere, at der er ført tilsyn med underdatabehandlere. Selvom Databehandleren er ansvarlig for at føre tilsyn med underdatabehandlere, har den Dataansvarlige eller dennes repræsentant adgang til at føre tilsyn med underdatabehandlere, når der efter den Dataansvarliges saglige vurdering opstår et behov herfor.

8. Underretningspligt og assistance

8.1. Databehandleren forpligter sig til uden unødig forsinkelse skriftligt at orientere den Dataansvarlige om afvigelser fra Databehandleraftalen, f.eks.:

i. Ved enhver fravigelse fra givne instrukser
ii. Ved enhver afvigelse fra det aftalte om tilgængelighed til personoplysninger omfattet af Databehandleraftalen.
iii. Ved planlagte releases, opgraderinger, tests mv., som er relevant for behandlingen af personoplysninger omfattet af Databehandleraftalen.
iv. Ved enhver begrundet mistanke om brud på fortroligheden, misbrug, fortabelse og forringelse af personoplysninger mv.

8.2. Databehandleren underretter uden unødig forsinkelse den Dataansvarlige efter at være blevet opmærksom på, at der er sket brud på persondatasikkerheden hos Databehandleren eller hos dennes eventuelle underdatabehandlere, der har tilknytning til Databehandleraftalen.

En underretning om brud på persondatasikkerheden skal indeholde følgende oplysninger:

i. Karakteren af bruddet på datasikkerheden og, hvis det er muligt, hvem der er omfattet, antal berørte og antal berørte registreringer af personoplysninger.
ii. Beskrivelse af de sandsynlige konsekvenser af bruddet.
iii. Beskrivelse af de foranstaltninger Databehandleren har truffet eller foreslår truffet for at håndtere databruddet og hvad der kan gøres for at begrænse dets mulige skadevirkninger.

8.3. Databehandleren skal uden unødig forsinkelse under hensyntagen til behandlingens karakter, så vidt muligt bistå den Dataansvarlige ved hjælp af passende tekniske og organisatoriske foranstaltninger, med opfyldelse af den Dataansvarliges forpligtelse til at besvare anmodninger om udøvelse af de registreredes rettigheder, som fastlagt i Databeskyttelsesforordningens kapitel 3.

8.4. Databehandleren skal assistere den Dataansvarlige med at overholde forpligtelser, der måtte påhvile den Dataansvarlige efter gældende ret, og hvor assistance er nødvendig for, at den Dataansvarlige kan overholde disse forpligtelser, herunder forpligtigelsen til at gennemføre en konsekvensanalyse vedrørende databeskyttelse.

9. Aftalens ikrafttræden og varighed

9.1. Databehandleraftalen træder i kraft ved underskrift fra alle parter.

9.2. Databehandleraftalen er gældende, så længe behandlingen af personoplysninger består og skal forblive i kraft frem til behandlingen er ophørt.

9.3. Databehandleren og dennes underdatabehandlere forpligter sig til at tilbagelevere og/eller slette personoplysninger, når databehandlingen i henhold til Hovedaftalen ophører eller på skriftlig anmodning fra den Dataansvarlige. Den Dataansvarlige skal oplyse Databehandleren om det tidspunkt, hvor databehandlingen skal ophøre. Det påhviler herefter Databehandleren at tilbagelevere og/eller slette personoplysningerne efter anmodning fra den Dataansvarlige, samt at slette eksisterende kopier på det oplyste tidspunkt, medmindre EU-retten eller national ret foreskriver opbevaring af personoplysningerne.

10. Håndtering af personoplysninger efter aftalens ophør

10.1. Databehandleren er ansvarlig for, at sletning af personoplysningerne sker på en sådan måde, at det ikke er muligt at genskabe personoplysningerne. Databehandleren er ansvarlig for, at personoplysningerne også slettes fra backup samt hos eventuelle underdatabehandlere.

10.2. Når sletningen er foretaget, skal Databehandleren fremsende en skriftlig erklæring på, at personoplysningerne er slettet som aftalt.

10.3. Såfremt Databehandleren eller dennes underdatabehandlere i forbindelse med konkurs, likvidering eller lignende ophører med at behandle personoplysninger for den Dataansvarlige, skal alle personoplysningerne straks leveres tilbage til den Dataansvarlige på en måde, der gør det muligt for den Dataansvarlige at anvende disse fremadrettet. Herefter er Databehandleren, dennes konkursbo eller lignende forpligtet til effektivt at slette personoplysningerne fra egne systemer i overensstemmelse med ovenstående.

11. Ophørsassistance

11.1. Ved ophør, opsigelse eller ophævelse af Hovedaftalen eller Databehandleraftalen, er Databehandleren på den Dataansvarliges anmodning forpligtet til at levere ophørsassistance til den Dataansvarlige indtil (i) alle personoplysninger er overført til den Dataansvarlige i et almindelig anerkendt elektronisk format, og (ii) der er sket tilfredsstillende overdragelse af ydelserne beskrevet i Hovedaftalen til den Dataansvarlige eller en ny leverandør udpeget af den Dataansvarlige. Databehandleren skal fortsætte behandlingen af personoplysningerne og leveringen af ydelser i henhold til Hovedaftalen og Databehandleraftalen, indtil der er sket en sådan tilfredsstillende overførsel.

11.2. Databehandleren er efter anmodning fra den Dataansvarlige forpligtet til skriftligt at oplyse den Dataansvarlige om, hvordan Databehandleren vil overføre personoplysningerne og ydelserne under Hovedaftalen til den Dataansvarlige eller en ny leverandør, herunder eventuelle tekniske krav og forudsætninger, således, at den Dataansvarlige selv eller den nye leverandør kan overtage ydelserne beskrevet i

Hovedaftalen og behandlingen af personoplysninger. Databehandleren skal til enhver tid efter anmodning fra den Dataansvarlige kunne dokumentere og demonstrere for den Dataansvarlige, at overførslen af personoplysninger og ydelser kan ske inden for de af Databehandlerens angivne tidsrammer.

12. Personoplysninger omfattet af denne aftale er fortrolige

12.1. Databehandleren skal sikre, og efter anmodning fra den Dataansvarlige påvise, at de medarbejdere, underdatabehandlere, samarbejdspartnere, eksterne konsulenter og vikarer mfl., der er autoriseret til at behandle de i Databehandleraftalen omfattede personoplysninger, har forpligtet sig til fortrolighed eller er underlagt en passende lovbestemt tavshedspligt.

12.2. Det påhviler Databehandleren at informere medarbejdere, underdatabehandlere, samarbejdspartnere, eksterne konsulenter og vikarer mfl. om tavshedspligten.

12.3. Databehandleren skal sikre, at adgangen til personoplysninger omfattet af denne Databehandleraftale er begrænset til de medarbejdere, for hvem det er nødvendigt at behandle personoplysninger for at kunne opfylde Databehandlerens forpligtelser over for den Dataansvarlige. Adgangen til personoplysningerne skal derfor uden unødig forsinkelse lukkes ned, hvis autorisationen fratages eller udløber.

12.4. Databehandleraftalens forpligtelser om tavshedspligt og fortrolighed gælder også efter Hovedaftalens ophør.

13. Overdragelse

13.1. Databehandleren må ikke overdrage sine rettigheder og forpligtelser i henhold til denne Databehandleraftale uden den Dataansvarliges forudgående samtykke.

14. Misligholdelse

14.1. Udover hvad der måtte fremgå af nærværende afsnit 14, har den Dataansvarlige de misligholdelsesbeføjelser, i forbindelse med Databehandlerens misligholdelse af Databehandleraftalen, der følger af dansk rets almindelige regler.

14.2. Databehandleraftalen er en del af Hovedaftalen, hvorved en misligholdelse af Databehandleraftalen også er en misligholdelse af Hovedaftalen. Ved væsentlig misligholdelse af Databehandleraftalen er den Dataansvarlige berettiget til at ophæve Databehandleraftalen og Hovedaftalen.

14.3. Den Dataansvarliges ophævelse af Hovedaftalen og Databehandleraftalen indebærer ikke, at den Dataansvarlige giver afkald på sin ret til at kræve erstatning, hvis betingelserne herfor er opfyldt.

14.4. Såfremt den Dataansvarlige vælger ikke at ophæve Hovedaftalen og Databehandleraftalen i ét eller flere tilfælde, selvom den Dataansvarlige er

berettiget hertil, medfører dette ikke, at den Dataansvarlige mister retten til at ophæve Hovedaftalen og Databehandleraftalen i andre tilfælde.

14.5. Den Dataansvarlige og Databehandleren er erstatningsansvarlige i overensstemmelse med dansk rets almindelige regler i tilfælde af misligholdelse af Databehandleraftalen eller overtrædelse af den til enhver tid gældende Databeskyttelseslovgivning.

Såfremt den Dataansvarlige af tredjemand gøres erstatningsansvarlig som følge af Databehandlerens eller eventuelle Underdatabehandleres misligholdelse af Databehandleraftalen eller overtrædelse af den til enhver tid gældende Databeskyttelseslovgivning, skal Databehandleren holde den Dataansvarlige skadesløs for alle omkostninger og tab.

Enhver ansvarsbegrænsning eller erstatningsmaksimering, der er fastlagt i Hovedaftalen eller andet sted, skal ikke være gældende i tilfælde af Databehandlerens misligholdelse af Databehandleraftalen eller den til enhver tid gældende Databeskyttelseslovgivning.

For kompensation og andre beløb der skal betales til de registrerede som følge af overtrædelse af Databeskyttelseslovgivningen, finder Databeskyttelsesforordningens artikel 82 anvendelse.

Databehandlerens forpligtelse til at skadesløsholde den Dataansvarlige efter nærværende afsnit gælder ikke for bøder eller sanktioner, der endeligt er pålagt den Dataansvarlige i medfør af Databeskyttelsesforordningens artikel 83 eller artikel 84.

14.6. Den Dataansvarlige er berettiget til at stille krav om, at Databehandleren bistår med at forsvare den Dataansvarliges interesser i en eventuel rets- eller voldgiftssag, uagtet Databehandlerens eventuelle indsigelser i forhold til den påberåbte misligholdelse, såfremt Databehandlerens bistand er af væsentlig betydning for varetagelsen af den Dataansvarliges interesser, og at dette ikke samtidig skader Databehandlerens stilling.

15. Lovvalg og værneting

15.1. Bestemmelserne i dette afsnit finder ikke anvendelse, såfremt lovvalg og værneting er særskilt reguleret i Hovedaftalen.

15.2. Databehandleraftalen inklusiv ethvert spørgsmål om Databehandleraftalens gyldighed er undergivet dansk ret.

15.3. Forhandling
Såfremt der opstår en uoverensstemmelse mellem Parterne i forbindelse med Databehandleraftalen, skal Parterne med en positiv, samarbejdende og ansvarlig holdning søge at indlede forhandlinger med henblik på at løse tvisten.

Enten:

15.4. Voldgift

Hvis enighed ikke kan opnås via forhandling eller på anden vis, skal tvisten løses ved voldgift.

Tvisten skal løses ved Voldgiftsinstituttet, The Danish Institute of Arbitration, efter de af instituttet vedtagne regler herom, som er gældende ved indledningen af voldgiftssagen.

Eller:

15.5. Domstolsbehandling

Hvis enighed ikke kan opnås via forhandling eller på anden vis, skal tvisten løses ved de danske domstole ved den Dataansvarliges hjemting.

16. Ændringer til punkterne 1-15

16.1. Det har været nødvendigt at foretage følgende ændringer i Databehandleraftalen [indsæt punktnummeret]

17. Bilag

Bilag 1: Databehandlerinstruks

Bilag 2: Underdatabehandler til Databehandleren

Eventuelle yderligere bilag

18. Underskrifter

På vegne af den Dataansvarlige:
Navn:
Stilling:
Adresse:

Dato:

Underskrift:

Den Dataansvarliges projektansvarlige/systemejers kontaktperson:
Navn:
Stilling:

Dato:

Underskrift:

På vegne af Databehandleren:
Navn:
Stilling:
Adresse:

Dato:

Underskrift:

Bilag 1 – Databehandlerinstruks

Ad. 2. Databehandlerens ansvar

2.2 Databehandling omfattet af Databehandleraftalen skal ske i overensstemmelse med denne instruks.

Ad. 3. Databehandlerens opgave

3.6 Ad hoc arbejdspladser

3.6.1 Der skal anvendes 2-faktor-autentifikation. Autentifikationsmetoden kan f.eks. være Nem-id, SMS-token, Rfid eller lignende.

3.6.2 Der må kun etableres eksterne IT-kommunikationsforbindelser, hvis der efter nærmere aftale herom træffes foranstaltninger til at sikre, at uvedkommende ikke gennem disse forbindelser kan få adgang til personoplysninger.

3.6.3 Databehandler skal efterleve Dataansvarliges retningslinjer for brug af ad hoc arbejdspladser.

Ad. 4. Tekniske og organisatoriske sikkerhedsforanstaltninger

4.1 Databehandleren skal som minimum træffe de nedenfor beskrevne tekniske og organisatoriske sikkerhedsforanstaltninger i forbindelse med behandlingen af personoplysninger omfattet af Databehandleraftalen.

4.1.1 Såfremt mere omfattende tekniske og organisatoriske sikkerhedsforanstaltninger er nødvendige for at sikre efterlevelse af Databehandleraftalens punkt 4, skal sådanne foranstaltninger altid træffes.

4.2 <u>Risici for sikkerhed</u>

4.2.1 Databehandleren skal tage de nødvendige skridt til at identificere, vurdere og begrænse enhver, med rimelighed forudsigelig, intern og ekstern risiko for tilgængeligheden, fortroligheden, og/eller integriteten af alle personoplysninger omfattet af Databehandleraftalen.

4.2.2 Databehandleren skal have passende tekniske foranstaltninger til at begrænse risikoen for enhver uautoriseret adgang. Databehandleren skal evaluere og forbedre effektiviteten af sådanne forholdsregler, når det er nødvendigt.

4.2.3 Databehandleren skal dokumentere de identificerede risici og hvordan risikoen er nedbragt til et acceptabelt niveau.

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.

4.2.4 Databehandleren skal have formelle procedurer for håndtering af sikkerhedshændelse.

4.3. Autorisation og adgangskontrol

4.3.1 Autorisationer skal angive, i hvilket omfang brugeren må forespørge, inddatere eller slette personoplysninger.

4.3.2 Kun de personer som autoriseres dertil, må have adgang til de personoplysninger, der behandles i henhold til Databehandleraftalen.

4.3.3 Databehandleren skal kunne dokumentere hvilke medarbejder der har autorisation til at tilgå personoplysninger, der behandles i henhold til Databehandleraftalen.

4.3.4 Autoriserede personer skal kunne fremvise billed-id ved on-site databehandling hos Dataansvarlig.

4.3.5 Der må kun autoriseres personer, der er beskæftiget med de formål, hvortil personoplysningerne behandles. De enkelte brugere må ikke autoriseres til anvendelser, som de ikke har brug for.

4.3.6 Der må endvidere autoriseres personer, for hvem adgang til personoplysningerne er nødvendig med henblik på revision eller drifts- og systemtekniske opgaver.

4.3.7 Den autoriserede bruger udstyres med en personlig brugeridentifikation og et personligt password, der skal anvendes hver gang, brugerne får adgang til databehandlingen. Passwords skal skiftes hvert halve år. Passwords skal have en tilstrækkelig længde og kompleksitet. Som udgangspunkt anvendes 2 faktor-autentifikation ved adgang til systemer med følsomme personoplysninger via internettet eller andet usikkert netværk. Autentifikationsmetoden kan f.eks. være Nem-id, SMS-token, Rfid eller lignende.

4.3.8 Databehandleren skal træffe foranstaltninger til at sikre, at kun autoriserede brugere kan få adgang til de personoplysninger, som den pågældende er autoriseret til.

4.3.9 Databehandleren skal have rimelige restriktioner for fysisk adgang. Områder hvor der sker behandling af personoplysninger i henhold til Hovedaftalen, skal være effektivt adskilt fra områder, hvortil der er generel adgang.

4.3.10 Databehandleren skal have formelle procedurer for håndtering af nulstilling af adgangskoder og for andre situationer, hvor den normale logiske adgangskontrol sættes ud af kraft.

4.3.11 Der skal løbende og mindst en gang hvert halve år foretages kontrol af, om brugerne er tildelt de adgange og autorisationer, som de bør have. Denne kontrol kan f.eks. indebære, at der i systemerne dannes en statistik over den enkelte brugers anvendelse af systemet, så det kan konstateres, om udstedte adgange og autorisationer fortsat anvendes.

4.3.12 Databehandleren skal uden unødig forsinkelse inddrage autorisationer og adgange for brugere, der efter en konkret vurdering ikke længere bør have disse.

4.4. Uddannelse og instruktion

4.4.1 Databehandleren skal sørge for, at dennes medarbejdere modtager den tilstrækkelige uddannelse og instruktioner for at sikre, at personoplysninger behandles i overensstemmelse med relevant lovgivning samt Databehandlerens politikker og procedurer herfor.

4.5. Kontrol med afviste adgangsforsøg og logning

4.5.1 Der skal foretages registrering af alle afviste adgangsforsøg. Hvis der inden for en fastsat periode er registreret højst 3 på hinanden følgende afviste adgangsforsøg med samme brugeridentifikation, skal der blokeres for yderligere forsøg fra denne brugeridentifikation. Adgangen åbnes først, når årsagen til afviste adgangsforsøg er klarlagt.

4.5.2 Der skal foretages maskinel registrering (logning) ved al behandling af personoplysninger. Loggen skal mindst indeholde oplysninger om tidspunkt, bruger, type af anvendelse og angivelse af den person, de anvendte oplysninger vedrørte eller det anvendte søgekriterium. Loggen skal opbevares i seks måneder, hvorefter den skal slettes, medmindre der i overensstemmelse med loggens formål fastsættes en længere opbevaringsperiode, af hensyn til at kunne anvende den som værktøj til brug ved efterforskning.

4.6. Inddatamateriale

4.6.1 Inddatamateriale må kun anvendes af personer, som er beskæftiget med inddateringen. Inddatamateriale skal opbevares på en sådan måde, at uvedkommende ikke kan gøre sig bekendt med de personoplysninger, der er indeholdt heri.

4.6.2 Når det ikke længere er nødvendigt at bevare inddatamaterialet, skal Databehandleren slette eller tilintetgøre inddatamaterialet. Fremgangsmåden herfor skal ske efter best practice.

4.6.3 Bestemmelsen vedrørende sletning eller tilintetgørelse gælder ikke, såfremt materialet er omfattet af bevarings-/kassationsbestemmelser i henhold til anden lovgivning, eller hvis journaliseret materiale behandles efter de almindelige arkivbestemmelser om bevaring, herunder aflevering af arkivalier til Statens Arkiver.

4.7. Uddatamateriale

4.7.1 Uddatamateriale er omfattet af samme instrukser som inddatamateriale med følgende tilføjelse:

4.7.2 Uddata må kun anvendes af personer, der er beskæftiget med de formål, til hvilke behandlingen af personoplysningerne foretages, samt i forbindelse med revision, teknisk vedligeholdelse, driftsovervågning og fejlretning mv.

4.8. Mobile lagringsmedier

4.8.1 Mobile lagringsmedier med personoplysninger skal være mærket, og skal opbevares med en tilstrækkelig stærk kryptering og under opsyn- eller under lås, når de ikke benyttes.

4.8.2 Mobile lagringsmedier med personoplysninger må kun udleveres til autoriserede personer med henblik på revision eller drifts- og systemtekniske opgaver.

4.8.3 Der skal føres en fortegnelse over hvilke mobile lagringsmedier, der benyttes i forbindelse med databehandlingen.

4.8.4 Der skal udarbejdes skriftlige instrukser for anvendelse og opbevaring af udtagelige mobile lagringsmedier.

4.8.5 I forbindelse med reparation og service af dataudstyr, der indeholder personoplysninger, samt ved salg og kassation af anvendte datamedier skal der træffes fornødne foranstaltninger for at sikre, at personoplysningerne ikke hændeligt eller bevidst tilintetgøres, fortabes eller forringes eller, at personoplysningerne kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med gældende lov. Dette skal ske efter best practice.

4.9. Sikkerhedskopier

4.9.1 Der gælder de samme retningslinjer for sikkerhedskopier som for al anden behandling af personoplysninger i medfør af denne aftale.

4.9.2 Databehandleren skal sikre, at systemer og personoplysninger sikkerhedskopieres regelmæssigt.

4.9.3 Sikkerhedskopier skal opbevares adskilt fra serveren i et ikke tilstødende rum for at sikre, at disse ikke går tabt f.eks. som følge af brand eller oversvømmelse. Opbevaring af sikkerhedskopier skal altid ske på betryggende vis så de ikke fortabes.

4.9.4 Databehandleren skal regelmæssigt kontrollere, at sikkerhedskopier er læsbare. Dette skal blandt andet gøres ud fra et beredskabssynspunkt, f.eks. ved større ændringer af et systems tekniske setup.

4.10. Opdateringer og ændringer

4.10.1 Databehandleren skal have formelle procedurer til sikring af, at opdateringer til operativsystemer, databaser, applikationer og anden software bliver vurderet og implementeret inden for rimelig tid.

4.10.2 Databehandleren skal have formelle procedurer for ændringshåndtering med henblik på at sikre, at enhver ændring er behørigt autoriseret, testet og godkendt inden implementering. Proceduren skal understøttes af en effektiv funktionsadskillelse eller ledelsesopfølgning med henblik på at sikre, at ingen enkeltpersoner kan implementere en ændring alene.

4.11. Driftsafbrydelser

4.11.1 Databehandleren skal have dokumenterede beredskabsprocedurer, der sikrer genetablering af services inden for rimelig tid i tilfælde af driftsafbrydelser.

4.12. Bortskaffelse af udstyr

4.12.1 Databehandleren skal have formelle processer i overensstemmelse med best practice og Dataansvarliges krav med henblik på at sikre, at der sker effektiv sletning af personoplysninger inden bortskaffelse af elektronisk udstyr.

4.12.2 Ved bortskaffelse af udstyr skal Databehandleren dokumentere fremgangsmåden herfor, og kunne forevise denne dokumentation efter anmodning herom.

4.13 Tilsyn

4.13.1 Databehandleren skal føre og dokumentere et tilsyn med Databehandlerens organisations overholdelse af lovkrav, politikker, procedurer og denne Databehandleraftale med bilag.

Ad. 8. Underretning og assistance

8.2 Ved brud på persondatasikkerheden skal den Dataansvarlige uden unødig forsinkelse skriftligt orienteres på nedenstående adresse, således at den Dataansvarlige kan indberette bruddet til Datatilsynet og om nødvendigt underrette de registrerede. Underretningen skal ske til:

Region indsæt region
indsæt mail-adresse

Bilag 2 - Underdatabehandler til Databehandleren

Databehandleren anvender følgende underdatabehandler(e), i forbindelse med de opgaver, som Databehandleren udfører på vegne af den Dataansvarlige. Med indgåelse af Databehandleraftalen har den Dataansvarlige godkendt brugen af denne underdatabehandler.

Der udfyldes ét bilag pr. underdatabehandler.

Underdatabehandler	
Virksomhedens fulde navn	
CVR-nummer (eller tilsvarende)	
Virksomhedens adresse (inkl. land)	
Øvrige adresser hvorfra der behandles personoplysninger	
Kontaktperson hos underdatabehandler	
Har Databehandleren en aftale med underdatabehandleren, som opfylder kravene i Databehandleraftalen?	
Databehandling(er), som underdatabehandler deltager i	
Kategorier af personoplysninger som underdatabehandler behandler	

Overførsel af personoplysninger til tredjelande	
Foretager underdatabehandleren behandling af personoplysninger i et tredjeland?	
Hvis ja, angiv samtlige tredjelande	
Hvis ja, angiv overførselsgrundlaget (f.eks. en EU-standardkontrakt eller Binding Corporate Rules)	