BILAG 2.3
DATABEHANDLERAFTALE

Denne databehandleraftale ("**Databehandleraftale**") er indgået mellem Parterne i Samarbejdsaftalen, og med de definitioner for Parterne, som anvendes i Samarbejdsaftalen.

BAGGRUND OG INDLEDNING

- Parterne har indgået en aftale om samarbejde ("**Samarbejdsaftalen**"), og som bilag til Samarbejdsaftalen gælder hermed denne Databehandleraftale, som alle Parter er gjort bekendt med.

- Databehandleraftalen fastsætter de rettigheder og forpligtelser, som finder anvendelse, når en Part fungerer som Databehandler og foretager behandling af personoplysninger på vegne af en anden Part, der har rolle som Dataansvarlig. Databehandleraftalen er udformet med henblik på Parternes efterlevelse af artikel 28, stk. 3 i Databeskyttelsesforordningen.

- Det er vedlagt tre bilag til Databehandleraftalen, der fungerer som integrerede dele af Databehandleraftalen:
  - Bilag 2.2 indeholder den Dataansvarliges instruks til Databehandleren om, hvilken behandling der skal foretages, og den type af Persondata, som Behandlingen omfatter.
  - Bilag 6.1 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.
  - Bilag 7.2 indeholder en beskrivelse af Databehandlerens sikkerhedsforanstaltninger.

1 DEFINITIONER OG FORTOLKNING

1.1 Listen nedenfor angiver definitionen af de oplistede begreber, der anvendes i Databehandleraftalen. Uanset, at en definition er angivet i ental, omfatter definitionen også flertal og omvendt. Henvisninger til bilag, afsnit og underafsnit skal forstås som henvisninger til bilag, afsnit og underafsnit i Databehandleraftalen medmindre andet fremgår udtrykkeligt eller er åbenlyst ud fra konteksten.

Behandling	betyder enhver aktivitet eller række af aktiviteter som Persondata gøres til genstand for, hvad end aktiviteten sker med eller uden brug af automatisk behandling og kan omfatte overførelse af Persondata til ethvert land inden for EU og inden for Det Europæiske Økonomiske Samarbejdsområde såvel som lande, der anses for at have et tilsvarende beskyttelsesniveau.
Dataansvarlig	betyder den fysiske eller juridiske person, offentlige myndighed, institution eller et andet organ, der alene eller sammen med andre afgør til hvilke formål og med hvilke hjælpemidler der må foretages Behandling af Personoplysninger.
Databehandler	betyder den fysiske eller juridiske person, offentlige myndighed, institution eller et andet organ, der behandler Personoplysninger på den Dataansvarliges vegne.

Databeskyttelses-forordningen	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
Datasubjekt	betyder den fysiske person, hvis Persondata bliver Behandlet.
Gældende Ret	betyder enhver af følgende reguleringer i det omfang de er anvendelige overfor en Part: enhver vedtægt, forordning, lovgivning, primær eller sekundær regulering, inklusiv gældende dansk ret, for tiden Lov nr. 502 af 23. maj 2018 om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (databeskyttelsesloven) samt Databeskyttelsesforordning, for tiden 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 mv. (databeskyttelsesforordningen), enhver bindende retsafgørelse eller dom, enhver anvendelig branchesædvane, politik eller standard, der kan håndhæves ved lov samt anvendelige anvisninger, politikker, krav, regler eller ordrer, som er udstedt af en myndighed.
Persondata	betyder enhver form for information om en identificeret eller identificerbar fysisk person (Datasubjektet); ved identificerbar fysisk person forstås en fysisk person, der direkte eller indirekte kan identificeres, navnlig ved en identifikator som defineret i Persondataforordningen, og som er indsamlet af den Dataansvarlige, Databehandleren eller af en hvilken som helst af disses virksomheders filialer, repræsentanter eller lignende.
Særlige kategorier af Persondata	betyder oplysninger om race eller etnisk oprindelse, politisk, religiøs eller filosofisk overbevisning eller fagforeningsmæssigt tilhørsforhold, genetiske data, helbredsoplysninger eller oplysninger om en fysisk persons seksuelle forhold eller seksuelle orientering samt oplysninger i form af biometriske data, såfremt biometriske data behandles med det formål entydigt at identificere en fysisk person (følsomme oplysninger).
Sikkerhedsbrud	betyder et brud på sikkerheden, der fører til hændelig eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet.
Tredjelande	betyder ethvert land uden for anvendelsesområdet for Databeskyttelsesforordningen i Det Europæiske Økonomiske Samarbejdsområde (EØS), med undtagelse af godkendte lande som Europa Kommissionen fra tid til anden vurderer, har en tilstrækkelig beskyttelse af Persondata.

Underdatabehandler	betyder en underleverandør, der er udpeget af Databehandleren til at behandle Persondata på vegne af den Dataansvarlige under instruktion af Databehandleren.
Ydelser	betyder de Ydelser som Databehandleren skal levere til den Dataansvarlige, eller som Underdatabehandleren skal levere til Databehandleren i henhold til Samarbejdsaftalen.

1.2 Bilagene til Databehandleraftalen udgør en integreret del af Databehandleraftalen og skal tillægges retskraft herefter, og enhver reference til Databehandleraftalen omfatter bilagene.

1.3 En reference til "på skrift" eller "skriftlig" betyder e-mail.

1.4 Overskrifterne i Databehandleraftalen er indsat for overskuelighedens skyld og til brug for referencer. Overskrifterne skal ikke påvirke betydningen eller fortolkningen af Databehandleraftalen.

2 UDPEGNING AF DATABEHANDLER

2.1 En Part udpeger en anden Part som Databehandler i relation til denne Databehandleraftale, i de situationer, hvor Parten behandler Persondata på vegne af den anden Part og efter Partens instruks.

2.2 I tilfælde af, at en af Parterne bliver udpeget til at være databehandler for en tredjepart, kan denne Databehandleraftale benyttes som grundlag for, at Databehandleren udpeges som Underdatabehandler. Tredjeparten bliver i det tilfælde dataansvarlig, og Databehandleraftalens Dataansvarlige bliver til databehandler, og Databehandleraftalens Databehandler bliver underdatabehandler.

2.3 Databehandleren behandler herefter Persondata efter instruks fra den Dataansvarlige. Denne instruks fremgår nærmere af bilag 2.2. Parterne oplyser og indestår for, at den Persondata, der Behandles i henhold til Databehandleraftalen, er proportionel med Parternes formål. Yderligere oplysninger, datakategorier og Datasubjekter mv. findes i bilag 2.32.2, der kan ændres af Parterne ved skriftlig fremsendelse af en opdateret version af bilaget.

3 FORPLIGTELSER VEDRØRENDE BEHANDLING OG BESKYTTELSE AF PERSONDATA

3.1 Den Dataansvarlige er ansvarlig for at sikre, at der er hjemmel til den Behandling af Persondata, som Databehandleren bliver instrueret i at foretage.

3.2 Databehandleren behandler både almindelig og følsom Persondata, og Databehandleren bekræfter, at oplysningerne behandles strengt fortroligt. Databehandleren må kun Behandle Persondata for at opnå formålet beskrevet i Samarbejdsaftalen og i henhold til instruksen vedlagt som bilag 2.32.2. Databehandleren sikrer desuden, at de personer, der er ansat hos Databehandleren, og som Behandler Persondata, har forpligtet sig til fortrolighed eller er underlagt en passende lovbestemt tavshedspligt.

3.3 Databehandleren bekræfter til enhver tid at Behandle Persondata i overensstemmelse med Gældende Ret samt anden privatlivs- eller databeskyttelsesregulering og udelukkende til det formål og på den måde, som den Dataansvarlige skriftligt har instrueret Databehandleren i. Databehandleren må ikke Behandle Persondata på nogen anden måde eller til nogen andre formål. Dette betyder, at Databehandleren ikke har indflydelse på formålet med og vilkårene

for Behandlingen af Persondata, og Databehandleren kan ikke træffe beslutninger om, hvorledes den modtagne Persondata skal anvendes, hvorvidt Persondata skal overdrages til tredjeparter, eller hvor længe Persondata skal opbevares.

3.4 Gældende Ret forpligter den Dataansvarlige til at sørge for, at Databehandleren stiller de fornødne garantier for, at Databehandleren har eller vil gennemføre passende tekniske og organisatoriske sikkerhedsforanstaltninger for at forhindre uautoriseret eller ulovlig Behandling, utilsigtet tab, ødelæggelse eller beskadigelse af Persondata, jf. Databehandleraftalens punkt 7, ligesom Gældende Ret forpligtiger den Dataansvarlige til at sikre, at disse foranstaltninger overholdes. Parterne er enige om, at beskyttelsen af privatlivet og sikkerheden omkring den Persondata, der behandles, skal tillægges stor betydning.

3.5 Når den Dataansvarlige anmoder herom, skal Databehandleren så vidt muligt stille nødvendige oplysninger til rådighed for den Dataansvarlige, således at den Dataansvarlige kan afgøre om passende tekniske og organisatoriske sikkerhedsforanstaltninger er indarbejdet, herunder procedurer for håndtering af krav om ændringer, tilføjelser, bortskaffelse af eller beskyttelse af Persondata, procedurer for eventuelle brud på sikkerheden, samt gennemførelse af en konsekvensanalyse og gennemførte ændringer som følge af berettigede indsigelser. Derudover skal Databehandleren give mulighed for og bidrage til revisioner, herunder inspektioner af Databehandlerens forhold, sikkerhedsforanstaltninger og Behandlinger, jf. Databehandleraftalens punkt 8, uanset om sådanne foretages af den Dataansvarlige eller en tredjemand, som er bemyndiget hertil af den Dataansvarlige.

3.6 Når Databehandleren modtager en forespørgsel fra et Datasubjekt, en myndighed eller en tredjepart om en Behandling, skal Databehandleren meddele den Dataansvarlige herom hurtigst muligt og senest inden for otteogfyrre (48) timer efter modtagelsen af forespørgslen. Databehandleren skal samtidig oplyse den Dataansvarlige om enhver relevant information vedrørende forespørgslen. Databehandleren besvarer ikke henvendelser uden at have fået skriftligt samtykke fra den Dataansvarlige, medmindre der foreligger et lovligt grundlag, som for eksempel ved forespørgsler fra politiet.

3.7 Databehandleren skal og vil sikre at enhver tredjepart, der leverer ydelser til Databehandleren, og som kommer i berøring med Persondata overholder de relevante vilkår i Databehandleraftalen, herunder de regler for opbevaring af Persondata, som Parterne fastsætter fra tid til anden, som er beskrevet i instruksen i bilag 2.2. Aftaler med tredjeparter skal være skriftlige.

4 BISTAND TIL DEN DATAANSVARLIGE

4.1 Under hensyntagen til Behandlingens karakter, bistår Databehandleren så vidt muligt den Dataansvarlige ved hjælp af passende tekniske og organisatoriske foranstaltninger, jf. hertil Databehandleraftalens punkt 7, med opfyldelse af den Dataansvarliges forpligtelse til at besvare anmodninger om udøvelsen af Datasubjekters rettigheder i henhold til Gældende Ret.

4.2 Dette indebærer, at Databehandleren så vidt muligt skal bistå den Dataansvarlige i forbindelse med den Dataansvarliges overholdelse af:

a. oplysningspligten ved indsamling af Persondata hos Datasubjektet

b. oplysningspligten, hvis Persondata ikke er indsamlet hos Datasubjektet

c. Datasubjektets indsigtsret

d. retten til berigtigelse og sletning

e. retten til begrænsning af Behandling

f. underretningspligt i forbindelse med berigtigelse eller sletning af Persondata eller begrænsning af Behandling

g. retten til dataportabilitet

h. retten til indsigelse

4.3 Derudover bistår Databehandleren den Dataansvarlige med at sikre overholdelse af den Dataansvarliges forpligtelser til blandt andet at

a. gennemføre en konsekvensanalyse vedrørende databeskyttelse, hvis en type Behandling sandsynligvis vil indebære en høj risiko for Datasubjekters rettigheder og frihedsrettigheder, og

b. høre tilsynsmyndigheden (Datatilsynet) inden en 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.

4.4 Parternes eventuelle aftale om vederlæggelse eller lignende i forbindelse med Databehandlerens bistand til den Dataansvarlige vil fremgå af Samarbejdsaftalen.

5 TREDJELANDE

5.1 Databehandleren må ikke Behandle Persondata udenfor Det Europæiske Økonomiske Samarbejdsområde uden først at indhente skriftlig tilladelse hertil fra den Dataansvarlige, som beskrevet i afsnit 6.1, medmindre den specifikke Behandling kræves i henhold til EU-ret, Gældende Ret eller medlemsstaternes nationale ret, som Databehandleren er underlagt. I dette tilfælde underretter Databehandleren den Dataansvarlige om det retlige krav inden Behandlingen påbegyndes, medmindre den pågældende ret forbyder en sådan underretning af hensyn til vigtige samfundsmæssige interesser.

5.2 Hvis den Dataansvarlige giver tilladelse til at Behandle Persondata udenfor Det Europæiske Økonomiske Samarbejdsområde, er en sådan tilladelse til Behandling i alle tilfælde betinget af, at Persondata bliver Behandlet i overensstemmelse med Gældende Ret samt i overensstemmelse med enhver anden instruktion som den Dataansvarlige giver vedrørende Behandlingen.

6 UNDERDATABEHANDLERE

6.1 Databehandleren er berettiget til at benytte Underdatabehandlere. De Underdatabehandlere, Databehandleren anvender på tidspunktet for indgåelsen af Databehandleraftalen, er oplistet i Databehandleraftalens bilag 6.16.1, hvor proceduren for godkendelse af Underdatabehandlere tillige fremgår. Databehandleren skal underrette den dataansvarlige om eventuelle planlagte ændringer vedrørende tilføjelse eller erstatning af andre Underdatabehandlere og derved give den Dataansvarlige mulighed for at gøre indsigelse mod sådanne ændringer.

6.2 Databehandleren skal sikre, at samtlige Underdatabehandlere skriftligt forpligter sig til at Behandle Persondata som beskrevet i denne Databehandleraftale, hvilket blandt andet betyder

at Underdatabehandleren på forespørgsel fra den Dataansvarlige skal give denne de nødvendige oplysninger for at den Dataansvarlige kan afgøre, om der er foretaget de påkrævede tekniske og organisatoriske sikkerhedsforanstaltninger, herunder procedurer omkring inspektion, procedure for at gennemføre ændringer og tilføjelser, bortskaffelse eller beskyttelse af Persondata samt oplysninger vedrørende gennemførte ændringer som følge af berettigede indsigelser.

7 SIKKERHEDSFORANSTALTNINGER

7.1 Databehandleren skal indarbejde alle passende tekniske og organisatoriske foranstaltninger for at beskytte Persondata imod utilsigtet tab samt enhver ulovlig Behandling. Under hensyntagen til disse foranstaltningers karakter og omkostningerne forbundet med implementering heraf, skal foranstaltningerne sikre et passende sikkerhedsniveau taget de risici, der er forbundet med Behandlingen af Persondata og disses karakter i betragtning. Sådanne foranstaltninger inkluderer altid som minimum foranstaltninger:

a) der sikrer en sikker overførelse af Persondata mellem Databehandleren og tredjeparter, der optræder som Underdatabehandlere ved udelukkende at bruge krypterede overførelsesprotokoller, som eksempelvis HTTPS eller SSL.

b) der sikrer, at det kun er autoriseret personale, der har adgang til Persondata til det aftalte formål, herunder foranstaltninger som begrænser adgangen til Persondata ved at oprette en liste, der specificerer, hvilke forudbestemte computere, baseret på IP-adresser, der har adgang til Persondata;

c) hvorved Databehandleren kun giver dets ansatte adgang til Persondata via sporbare konti, der kan spores ved navn og som ved brug bliver tilstrækkelig logget;

d) der sikrer Persondata imod uautoriseret og ulovlig opbevaring, Behandling, adgang eller offentliggørelse;

e) der systematiserer gentagne og periodiske procedurer vedrørende scanning, identifikation og afhjælpning af hidtil ukendte sikkerhedsproblemer på servere, arbejdsstationer, netværk, udstyr og applikationer;

f) hvis formål det er at identificere svagheder i relation til Behandling af Persondata i de systemer, der bliver brugt til at levere Ydelser til den Dataansvarlige.

7.2 En beskrivelse af Databehandlerens foranstaltninger er vedlagt som Databehandleraftalens bilag 7.2.

7.3 Databehandleren skal evaluere og forbedre de tekniske og organisatoriske foranstaltninger, som er indført, hvis kravene eller den teknologiske udvikling giver anledning hertil.

8 TILSYN OG ADGANG TIL REVISION

8.1 Databehandleren skal, når den Dataansvarlige fremsætter en begrundet anmodning herom, stille de nødvendige oplysninger til rådighed for den Dataansvarlige, således at den Dataansvarlige har mulighed for at danne sig et indtryk af, om og hvordan Databehandleren opfylder Databehandleraftalen. Dette omfatter oplysninger vedrørende de sikkerhedsforanstaltninger,

der refereres til i afsnit 7, oplysninger om backupprocedurer, (forsøg eller mistanke om) hacking, mv.

8.2 Såfremt Enhederne har aktiveret Databehandleraftalen mellem sig, således at en Part benytter en anden som Databehandler, skal Databehandleren selv eller en repræsentant for Databehandleren foretage et årligt tilsyn i hvert kalenderår vedrørende overholdelsen af denne Databehandleraftale. Der er mellem Parterne enighed om, at Databehandlerens egenkontrol skal udføres med udgangspunkt i vedlagte egenkontrolskema (bilag 8.2), der er opbygget på baggrund af og med indhold ligesom anerkendte revisionserklæringer, som ISO 27001 ISAE 3000 eller ISAE 3402. Dokumentation for den afholdte egenkontrol, inklusiv kontrolrapporten, skal snarest muligt sendes til orientering til den Dataansvarlige, dog senest én (1) måned efter udarbejdelsen.

8.3 Den Dataansvarlige eller en repræsentant for den Dataansvarlige har herudover adgang til at få foretaget revision af Databehandleren eller føre ekstraordinært tilsyn, herunder fysisk tilsyn, hos Databehandleren, hvis der efter den dataansvarliges vurdering opstår et behov herfor.

8.4 Den Dataansvarliges eventuelle udgifter i forbindelse med revision og tilsyn afholdes af den Dataansvarlige selv. Databehandleren er dog forpligtet til at afsætte de ressourcer og den tid, der er nødvendig for, at den Dataansvarlige kan gennemføre tilsyn.

8.5 Såfremt en tredjepart skal fortage tilsyn eller revision på vegne af den Dataansvarlige, skal den Dataansvarlige udarbejde en skriftlig fortrolighedsaftale med tredjeparten, inden denne gennemfører tilsynet eller revisionen.

8.6 **Underdatabehandlere**

8.6.1. Databehandleren eller en repræsentant for Databehandleren foretager desuden ét årligt tilsyn vedrørende overholdelsen af denne Databehandleraftale hos Underdatabehandlere efter samme vilkår, som nævnt ovenfor. Dokumentation for de afholdte tilsyn sendes snarest muligt til orientering hos den Dataansvarlige, dog senest én (1) måned efter indhentelsen.

8.6.2. På opfordring fra den Dataansvarlige skal Databehandleren indhente kontroloplysninger ud fra tilsvarende præmisser som beskrevet i afsnit 8.2 fra sine Underdatabehandlere og sende erklæringerne til den Dataansvarlige til orientering senest to (2) måneder efter indhentelsen.

8.6.3. Den Dataansvarlige kan, hvis den Dataansvarlige finder det nødvendigt, vælge at initiere og deltage på en fysisk inspektion hos Underdatabehandleren. Dette kan blive aktuelt, såfremt den Dataansvarlige vurderer, at Databehandlerens tilsyn med Underdatabehandleren ikke har givet den Dataansvarlige tilstrækkelig sikkerhed for, at Behandlingen hos Underdatabehandleren sker i overensstemmelse med denne Databehandleraftale.

8.6.4. Den Dataansvarliges eventuelle deltagelse i et tilsyn hos Underdatabehandleren ændrer ikke ved, at Databehandleren også herefter har det fulde ansvar for Underdatabehandlerens overholdelse af Gældende Ret og Databehandleraftalen.

8.7 **Retningslinjer for revision**

8.7.1. Ved den Dataansvarliges anmodning om revision, jf. afsnit 8.38.3, skal den Dataansvarlige indsende en detaljeret plan for den foreslåede revision senest fire (4) uger før den foreslåede dato for revisionen til Databehandleren, der beskriver det forventede omfang, varighed heraf, samt startdatoen for revisionen. Databehandleren skal herefter gennemgå planen for revision og oplyse den Dataansvarlige om eventuelle betænkninger eller spørgsmål hertil (eksempelvis hvis den Dataansvarlige anmoder om oplysninger, der kan kompromittere Databehandlerens forretning, sikkerhed, privatliv, ansættelsesforhold eller andre relevante politikker). Databehandleren og den Dataansvarlige skal i samarbejde blive enige om en endelig plan for revisionen.

8.7.2. Hvis der ønskes udført revision på et område, der er adresseret i en SSAE 16/ISAE 3000 eller ISAE 3402 Type 2, ISO, NIST, PCI DSS, HIPAA eller en lignende revisionsrapport, der er udført af en kvalificeret tredjepart inden for de seneste tolv (12) måneder, og Databehandleren bekræfter, at han ikke har kendskab til nogle materielle ændringer, der kan påvirke resultatet af den udførte revision, indvilliger den Dataansvarlige i at godkende disse resultater, i stedet for at anmode om en revision af de områder, der er omfattet af rapporten.

8.7.3. Revisionen skal udføres inden for almindelig åbningstid på det sted, der er genstand for Databehandlerens forpligtelser, og må ikke forstyrre Databehandlerens forretningsaktiviteter unødigt.

8.8 Enhver revision skal udføres for den Dataansvarliges regning. Såfremt den Dataansvarlige anmoder om assistance fra Databehandleren i forbindelse med revisionen, skal assistancen betragtes som en separat ydelse fra Databehandleren, hvis assistancen med revisionen kræver brug af interne, eksterne eller andre særlige ressourcer. Databehandleren skal indhente den Dataansvarliges skriftlige godkendelse og indgå aftale om betaling af eventuelle relaterede gebyrer, før der foretages en assistance med revisionen.

8.9 Den Dataansvarlige må kun bruge revisionsrapporterne med henblik på at opfylde sine retlige forpligtigelser vedrørende revision eller til at bekræfte, at kravene i Databehandleraftalen overholdes.

9 SIKKERHEDSBRUD

9.1 I tilfælde af et Sikkerhedsbrud skal Databehandleren uden unødig forsinkelse underrette den Dataansvarlige herom. Underretningen skal om muligt ske senest fireogtyve (24) timer efter, at Sikkerhedsbruddet er opdaget, sådan at den Dataansvarlige har mulighed for at efterleve sin eventuelle forpligtelse til at anmelde bruddet til tilsynsmyndigheden (Datatilsynet) inden for tooghalvfjerds (72) timer. Databehandleren skal ikke foretage anmeldelse af brud, der vedrører Persondata, som behandles for den Dataansvarlige.

9.2 Underretningen til den Dataansvarlige skal indeholde en beskrivelse af:

9.2.1 Sikkerhedsbruddets karakter og de foranstaltninger, som Databehandleren foreslår, at der tages, eller som Databehandleren allerede har taget for at begrænse de negative konsekvenser af Sikkerhedsbruddet,

9.2.2 kategorierne af Datasubjekter, det omtrentlige antal berørte Datasubjekter og det omtrentlige antal berørte registreringer af Persondata,

9.2.3 de konstaterede og de sandsynlige konsekvenser som Sikkerhedsbruddet har for Behandlingen af Persondata og de foranstaltninger, der er taget eller som foreslås taget af Databehandleren for at afhjælpe disse konsekvenser.

9.3 Så snart Databehandleren opdager et Sikkerhedsbrud, skal denne straks foretage de nødvendige foranstaltninger for at begrænse de negative konsekvenser af Sikkerhedsbruddet og for at forhindre gentagelse heraf.

9.4 Databehandleren har en databeredskabsplan, som tillader Databehandleren at informere den Dataansvarlige om Sikkerhedsbrud og videre tillader Parterne at arbejde effektivt sammen for at håndtere hændelsen.

9.5 Hvis den Dataansvarlige eller Databehandleren opdager et Sikkerhedsbrud, meddeler den dette til den anden Part, og begge Parter træffer alle de nødvendige foranstaltninger i overensstemmelse med Gældende Ret for at forhindre eller begrænse yderligere overtrædelser eller Sikkerhedsbrud i relation til Behandlingen af Persondata.

9.6 Hvis den Dataansvarlige er underlagt en pligt til at anmelde Sikkerhedsbruddet, skal Databehandleren assistere og vejlede den Dataansvarlige herom på forespørgsel fra den Dataansvarlige.

10 ANSVAR

10.1 Hvis Databehandleren ikke overholder sine forpligtelser eller på anden vis bryder Databehandleraftalen, som følge af Databehandlerens handlinger eller undladelser, er Databehandleren ansvarlig for bøder og direkte økonomiske tab lidt hos den Dataansvarlige.

10.2 Uanset afsnit 10.110.1 er Databehandleren aldrig ansvarlig for den Dataansvarliges handlinger og udeladelser. Endvidere er Databehandleren ikke ansvarlig for egne handlinger og udeladelser, hvis de er opstået som følge af Databehandlerens overholdelse af Gældende Ret.

10.3 I dette tilfælde vil den Dataansvarlige være berettiget til at kræve erstatning for tab og omkostninger afholdt som følge af den manglende overholdelse under forudsætning af, at Databehandlerens manglende overholdelse ikke skyldes den Dataansvarliges misligholdelse af Databehandleraftalen.

11 DIVERSE

11.1 Databehandleraftalen er gældende så længe Databehandleren leverer de beskrevne Ydelser i Samarbejdsaftalen til den Dataansvarlige eller Behandler Persondata på vegne af den Dataansvarlige.

11.2 Ved Databehandleraftalens udløb skal Databehandleren på opfordring stille en kopi af al Persondata, som Databehandleren har Behandlet på vegne af den Dataansvarlige, til rådighed for denne og på anmodning slette Persondata. Såfremt den Dataansvarlige ikke anmoder om at få en kopi af Persondataen, slettes al Persondata senest tre (3) måneder efter Databehandleraftalens ophør.

11.3 Databehandleraftalens punkt 11.1 og 11.2 har forrang overfor eventuelle tilsvarende bestemmelser i andre aftaler mellem Parterne, herunder i Samarbejdsaftalen.

11.4 Databehandleraftalen og Samarbejdsaftalen er indbyrdes afhængige og kan ikke opsiges særskilt. Databehandleraftalen kan dog – uden at opsige Samarbejdsaftalen – erstattes af en

anden gyldig databehandleraftale. Uanset opsigelse af Parternes aftaler, vil bestemmelserne i Databehandleraftalen forblive i kraft frem til, at Databehandleren har ophørt med Behandlinger af Persondata på vegne af den Dataansvarlige, og at Databehandleren og eventuelle Underdatabehandlere har slettet alt Persondata omfattet af Databehandleraftalen.

12 FORTROLIGHED

12.1 Enhver person, der er involveret i opfyldelsen af denne Databehandleraftale og som følge heraf opnår adgang til den Persondata, hvis fortrolige karakter vedkommende kender eller burde kende, og som ikke allerede som følge af deres stilling, deres profession eller lovbestemte regler er underlagt en fortrolighedspligt, er forpligtet til at bevare Persondataens fortrolighed.

12.2 Punkt 12.112.1 gælder ikke i de tilfælde, hvor vedkommende er forpligtet til at videregive de pågældende Persondata som følge af Gældende Ret eller på anden vis som beskrevet i punkt 13.1 nedenfor.

12.3 Fortrolighedspligten gælder også efter Databehandleraftalens ophør.

13 LOVPLIGTIG VIDEREGIVELSE

13.1 Medmindre andet er påkrævet i henhold til Gældende Ret, skal Databehandleren straks underrette den Dataansvarlige om alle retslige, administrative eller voldgiftsretlige kendelser fra et forvaltnings- eller administrationsorgan eller fra en offentlig myndighed som Databehandleren modtager, og som vedrører den Persondata som Databehandleren Behandler på vegne af den Dataansvarlige. Hvis den Dataansvarlige anmoder herom, skal Databehandleren give den Dataansvarlige de oplysninger, som Databehandleren har i sin besiddelse, som kan opfylde tredjepartens påkrav samt enhver rimelig efterspurgt assistance for, at den Dataansvarlige kan imødekomme et lignende påkrav inden for rimelig tid. Den Dataansvarlige anerkender, at Databehandleren ikke har ansvaret for at deltage direkte overfor den enhed, der måtte fremsætte krav herom.

14 MEDDELSER

14.1 Meddelelser, som afgives i medfør af Databehandleraftalen, skal sendes skriftligt pr. e-mail. Enhver aftale mellem Parterne skal indgås skriftligt, før aftalen er gyldig.

14.2 Parterne er forpligtet til løbende at orientere hinanden skriftligt om eventuelle ændringer i de oplyste kontaktpersoner.

15 LOVVALG OG VÆRNETING

15.1 Denne Databehandleraftale og enhver retlig tvist, der opstår i forbindelse med Databehandleraftalen (inklusiv tvister eller krav, der opstår uden for kontrakt) er underlagt dansk ret undtaget CISG og de international privatretlige regler.

15.2 Parterne er enige om, at Københavns Byret udgør værneting for enhver tvist eller krav, der opstår i forbindelse med denne Databehandleraftale eller indgåelse af samme (herunder ikke-kontraktretlige tvister eller krav).

Bilag 2.2

Instruks til Databehandler

Dette bilag udgør den Dataansvarliges instruktion til Databehandleren i forbindelse med Databehandlerens Behandling af Persondata for den Dataansvarlige.

1. BEHANDLING AF PERSONDATA

1.1 Formål med Behandlingen af Persondata er:

I visse situationer anvender Enhederne Korpset som Databehandler. Dette er i de tilfælde, hvor Enhederne har behov for bistand til Medlemsservice, arrangementer, opkrævning af kontingent, bistand ved juridiske og vedtægtsmæssige forhold, osv. Listen er ikke udtømmende, men det er klart for såvel Enhederne som Korpset, hvornår Korpset agerer som Databehandler.

I visse tilfælde anvender en Enhed en anden Enhed som Databehandler. Dette er i de tilfælde, hvor Enhederne går sammen om at lave arrangementer, har behov for bistand fra hinanden, osv. Listen er ikke udtømmende, men det er klart for de enkelte Enheder, hvornår en anden Enhed agerer som Databehandler.

Databehandleraftalen er indgået for at sikre overholdelse af gældende ret i forbindelse med, at en Part agerer som databehandler, og databehandler indeholder instruks, sikkerhedsregulering, mv. og for at regulere ansvar og roller i forhold til Korpsets behandling af Persondata på vegne af Enhederne samt Enheders behandling af Persondata på vegne af andre Enheder.

1.2 Datasubjekterne er:

a) Individer over og under 18 år, herunder bl.a. (men ikke begrænset til):
    a. Medlemmer og frivillige
    b. Pårørende

2. KATEGORIER AF PERSONDATA

Behandlingen af Persondata ***kan*** omfatte men er ikke begrænset til følgende:

2.1.1 Individer over og under 18 år

2.1.1.1. Medlemmer og frivillige

a) Almindelige Persondata: Navn, adresse, postnummer, by, mobilnummer, mailadresse, fødselsdato, køn, kontaktoplysninger på pårørende, registrerings- og kontonummer, medlemsnummer, billeder, spejdernavn, kursusaktivitet, funktioner, skole og klassetrin.
b) Følsomme Persondata: Helbredsoplysninger.
c) Fortrolige Persondata: CPR-nr. ved indhentelse af børneattester jf. Børneattestloven.

2.1.1.2. Pårørende

a) Almindelige Persondata: Navn, adresse, postnummer, by, mobilnummer, e-mailadresse og i nogle tilfælde registrerings- og kontonummer.

3. BEHANDLINGSSIKKERHED

3.1 Sikkerhedsniveauet hos Databehandleren skal afspejle, at der kan være tale om både simpel behandling af få almindelige personoplysninger eller behandling af en stor mængde følsomme data. Alt efter indholdet og omfanget af persondataen skal der etableres et tilstrækkeligt sikkerhedsniveau.

3.2 Databehandleren er berettiget og forpligtet til at træffe beslutninger om hvilke tekniske og organisatoriske sikkerhedsforanstaltninger, der skal anvendes for at skabe det nødvendige sikkerhedsniveau omkring denne Persondata, og skal som minimum gennemføre de foranstaltninger, som er aftalt med den Dataansvarlige, se bilag 7.2.

4. OPBEVARINGSPERIODE OG SLETNING

4.1 Det følger af Gældende Ret, at Persondata ikke må opbevares længere, end hvad der er nødvendigt for, at formålet med Behandlingen kan opfyldes. Derfor er Parterne enige om følgende:

4.2 Databehandleren skal slette al Persondata, så snart en af følgende begivenheder indtræder:

- under hensyntagen til Databehandleraftalens punkt 3.6, når Datasubjektet har anmodet om, at Persondata slettes, eller
- hvis denne Databehandleraftale ophører, uanset årsagen hertil, og sletningen ikke strider mod Gældende Ret.

4.3 Persondata opbevares hos Databehandleren, indtil den Dataansvarlige anmoder om at få denne slettet eller tilbageleveret eller indtil databehandleren ikke længere ser noget formål med opbevaringen.

5. OVERFØRSEL AF PERSONOPLYSNINGER TIL TREDJELANDE

5.1 Der overføres ikke Persondata til Tredjelande.

Bilag 6.1

Underdatabehandlere

Databehandleren må alene gøre brug af Underdatabehandlere efter forudgående specifik skriftlig godkendelse fra den Dataansvarlige.

Databehandlerens anmodning herom skal være den Dataansvarlige i hænde minimum en (1) måned før anvendelsen eller ændringen skal træde i kraft. Den Dataansvarlige skal herefter tage stilling til anmodningen inden for syv (7) dage. Den Dataansvarlige kan alene nægte godkendelse, såfremt den Dataansvarlige har rimelige og konkrete årsager hertil.

Godkendte Underdatabehandlere:

Navn og adresse	**CVR-nr.**	**Land**	**Databehandleren bistår med følgende:**
Reload A/S Suomisvej 2, 2. Sal 1927 Frederiksberg	31768500	Danmark	Hjemmeside/Gruppeweb
Spejdernes Medlemsservice I/S Wagnersvej 33 2450 København SV	35438874	Danmark	Datalagring
Spejdernes Administrationsfællesskab Arsenalvej 10 1436 København K.	31352894	Danmark	Administration

Den Dataansvarlige har ved Databehandleraftalens ikrafttræden specifikt godkendt anvendelsen af ovennævnte Underdatabehandlere til netop den Behandling, som er beskrevet ovenfor.

Databehandleren kan ikke – uden den Dataansvarliges specifikke og skriftlige godkendelse – anvende den enkelte Underdatabehandler til en anden Behandling end aftalt eller lade en anden Underdatabehandler foretage den beskrevne behandling.

Databehandleren kan endvidere ikke inddrage yderligere Underdatabehandlere, end der fremgår ovenfor, uden specifik godkendelse fra den Dataansvarlige.

Bilag 7.2

Sikkerhedsforanstaltninger

Parterne er enige om, at sikkerhedsniveauet afspejler de typer af Persondata, der behandles.

Databehandleren er berettiget og forpligtet til at træffe beslutninger om, hvilke tekniske og organisatoriske sikkerhedsforanstaltninger, der skal anvendes for at skabe det nødvendige (og aftalte) sikkerhedsniveau omkring oplysningerne. Databehandleren skal dog i alle tilfælde og som minimum gennemføre følgende foranstaltninger, som er aftalt med den Dataansvarlige, nemlig:

Såfremt at følsomme Persondata opbevares andre steder end steder som Parterne på forhånd er enige om, er det er krav, at de krypteres, ex. i form af, at der etableres kodeord på dokumenter og mapper.

Rettidigt at kunne genoprette tilgængeligheden af og adgangen til Persondata i tilfælde af en fysisk eller teknisk hændelse.

Sikre at der foreligger procedurer for regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske foranstaltninger til sikring af behandlingssikkerhed.

Adgang til data via internettet er sikret af individuelle passwords, begrænset til relevante personer og til enhver tid ajourført/opdateret.

Der er pr. 1/1-2019 krav om kryptering ved transmission af fortrolige og følsomme personoplysninger der sendes via e-mail.

Fysisk sikring af lokaliteter, hvor der behandles personoplysninger, eksempelvis låse på døre, skabe og skuffer og alarmsikring af (kontor)lokaler.