



Databehandleraftale udarbejdet efter Datatilsynets standardkontraktbestemmelser accepteret af Det Europæiske Databeskyttelsesråd

Standardkontraktbestemmelser

i henhold til artikel 28, stk. 3, i forordning 2016/679 (GDPR) med henblik på databehandlerens behandling af personoplysninger

mellem

GENERISK DATAANSVARLIG
GENERISK DANNET ADRESSE
Aalborg 9000
DK
CVR-nr.:
herefter den "Dataansvarlige"

og

BOARD OFFICE A/S
Vesterbro 21 B, 1.
9000 Aalborg
DK
CVR-nr.: 28966237
herefter "Databehandleren"

der hver især er en "Part" og sammen udgør "Parterne"

HAR AFTALT følgende standardkontraktbestemmelser ("Bestemmelserne") med henblik på at overholde GDPR og sikre beskyttelse af privatlivets fred og fysiske personers grundlæggende rettigheder og frihedsrettigheder.

1. Indholdsfortegnelse

2. Præambel.....

3. Den dataansvarliges rettigheder og forpligtelser.....

4. Databehandleren handler efter instruks

5. Fortrolighed

6. Behandlingssikkerhed.....

7. Anvendelse af underdatabehandlere

8. Overførsel til tredjelande eller internationale organisationer

9. Bistand til den Dataansvarlige

10. Underretning om brud på persondatasikkerheden.....

11. Sletning og returnering af oplysninger.....

12. Revision, herunder inspektion.....

13. Parternes aftale om andre forhold

14. Ikrafttræden og ophør.

15. Kontaktpersoner hos den Dataansvarlige og Databehandleren

Bilag A Oplysninger om behandlingen.....

Bilag B Underdatabehandlere

Bilag C Instruks vedrørende behandling af personoplysninger.....

Bilag D Parternes regulering af andre forhold.....

Bilag E Standardkontraktbestemmelser.....

2. **Præambel**

- 2.1 Disse bestemmelser fastsætter Databehandlerens rettigheder og forpligtelser, når denne foretager behandling af personoplysningerne på vegne af den Dataansvarlige.
- 2.2 Disse bestemmelser 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 ("GDPR").
- 2.3 I forbindelse med leveringen af BOARD-OFFICE & BOARD-PEOPLE behandler Databehandleren personoplysninger på vegne af den Dataansvarlige i overensstemmelse med disse Bestemmelser.
- 2.4 Bestemmelserne har forrang i forhold til eventuelle tilsvarende bestemmelser i andre aftaler mellem Parterne.
- 2.5 Der hører bilag til disse Bestemmelser, og bilagene udgør en integreret del af Bestemmelserne.
- 2.6 Bilag A indeholder nærmere oplysninger om behandlingen af personoplysninger, herunder om behandlingens formål og karakter, typen af personoplysninger, kategorierne af registrerede og varighed af behandlingen.
- 2.7 Bilag B indeholder den Dataansvarliges betingelser for Databehandlerens brug af underdatabehandlere og en liste af underdatabehandlere, som den Dataansvarlige har godkendt brugen af.
- 2.8 Bilag C indeholder den Dataansvarliges instruks for så vidt angår Databehandlerens behandling af personoplysninger, en beskrivelse af de sikkerhedsforanstaltninger, som Databehandleren som minimum skal gennemføre, og hvordan der føres tilsyn med databehandleren og eventuelle underdatabehandlere.
- 2.9 Bilag D indeholder bestemmelser vedrørende andre aktiviteter, som ikke er omfattet af Bestemmelserne.
- 2.10 Hvis standardkontraktbestemmelser som omhandlet i GDPR, artikel 46, stk. 2, litra c og d, udgør grundlag for overførsel af personoplysninger mellem den Dataansvarlige og Databehandleren til tredjelande som omhandlet i GDPR, kapitel V, er disse vedlagt i engelsk version som Bilag E og E1.
- 2.11 Bestemmelserne med tilhørende bilag skal opbevares skriftligt, herunder elektronisk, af begge Parter.
- 2.12 Disse Bestemmelser frigør ikke Databehandleren fra forpligtelser, som Databehandleren er pålagt efter GDPR eller enhver anden lovgivning.

3. **Den Dataansvarliges rettigheder og forpligtelser**

- 3.1 Den Dataansvarlige er ansvarlig for at sikre, at behandlingen af personoplysninger sker i overensstemmelse med GDPR (se GDPR, artikel 24), databeskyttelsesbestemmelser i anden EU-ret eller EU/EØS-medlemsstaternes nationale ret og disse Bestemmelser.
- 3.2 Den Dataansvarlige har ret og pligt til at træffe beslutning om, til hvilke(t) formål og med hvilke hjælpemidler, der må ske behandling af personoplysninger.
- 3.3 Den Dataansvarlige er ansvarlig for, blandt andet, at sikre, at der er et behandlingsgrundlag for behandlingen af personoplysninger, som Databehandleren instrueres i at foretage.

4. **Databehandleren handler efter instruks**

- 4.1 Databehandleren må kun behandle personoplysninger efter dokumenteret instruks fra den Dataansvarlige, medmindre det kræves i henhold til EU-ret eller EU-/EØS-medlemsstaternes nationale ret, som Databehandleren er underlagt. Denne instruks skal være specificeret i Bilag A og C. Efterfølgende instruks kan også gives af den Dataansvarlige, mens der sker behandling af personoplysninger, men instruksen skal altid være dokumenteret og opbevares skriftligt, herunder elektronisk, sammen med disse Bestemmelser.
- 4.2 Databehandleren underretter omgående den Dataansvarlige, hvis en instruks efter vedkommendes mening er i strid med GDPR eller databeskyttelsesbestemmelser i anden EU-ret eller EU-/EØS-medlemsstaternes nationale ret.

5. **Fortrolighed**

- 5.1 Databehandleren må kun give adgang til personoplysninger, som behandles på den Dataansvarliges vegne, til personer, som er underlagt Databehandlerens instruktionsbeføjelser, og som har forpligtet sig til fortrolighed eller er underlagt en passende lovbestemt tavshedspligt, og kun i det nødvendige omfang. Listen af personer, som har fået tildelt adgang, skal løbende gennemgås. På baggrund af denne gennemgang, kan adgangen til personoplysninger lukkes, hvis adgangen ikke længere er nødvendig, og personoplysningerne skal herefter ikke længere være tilgængelige for disse personer.
- 5.2 Databehandleren skal efter anmodning fra den Dataansvarlige kunne påvise, at de pågældende personer, som er underlagt Databehandlerens instruktionsbeføjelser, er underlagt ovennævnte tavshedspligt.

6. **Behandlingssikkerhed**

- 6.1 GDPR, artikel 32, fastslår, at den Dataansvarlige og Databehandleren, 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, gennemfører passende tekniske og organisatoriske

foranstaltninger for at sikre et beskyttelsesniveau, der passer til disse risici.

Den Dataansvarlige skal vurdere risiciene for fysiske personers rettigheder og frihedsrettigheder som behandlingen udgør og gennemføre foranstaltninger for at imødegå disse risici. Afhængig af deres relevans kan det omfatte:

- 6.1.1 Pseudonymisering og kryptering af personoplysninger
 - 6.1.2 evne til at sikre vedvarende fortrolighed, integritet, tilgængelighed og robusthed af behandlingssystemer og -tjenester
 - 6.1.3 evne til rettidigt at genoprette tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse
 - 6.1.4 en procedure for regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske foranstaltninger til sikring af behandlingssikkerhed.
- 6.2 Efter GDPR, artikel 32, skal Databehandleren – uafhængigt af den Dataansvarlige – også vurdere risiciene for fysiske personers rettigheder som behandlingen udgør og gennemføre foranstaltninger for at imødegå disse risici. Med henblik på denne vurdering skal den Dataansvarlige stille den nødvendige information til rådighed for Databehandleren, som gør vedkommende i stand til at identificere og vurdere sådanne risici.
- 6.3 Derudover skal Databehandleren bistå den Dataansvarlige med vedkommendes overholdelse af den Dataansvarliges forpligtelse efter GDPR, artikel 32, ved bl.a. at stille den nødvendige information til rådighed for den Dataansvarlige vedrørende de tekniske og organisatoriske sikkerhedsforanstaltninger, som Databehandleren allerede har gennemført i henhold til GDPR, artikel 32, og al anden information, der er nødvendig for den Dataansvarliges overholdelse af sin forpligtelse efter GDPR, artikel 32.

Hvis imødegåelse af de identificerede risici – efter den Dataansvarliges vurdering – kræver gennemførelse af yderligere foranstaltninger end de foranstaltninger, som Databehandleren allerede har gennemført, skal den Dataansvarlige angive de yderligere foranstaltninger, der skal gennemføres, i Bilag C.

7. **Anvendelse af underdatabehandlere**

- 7.1 Databehandleren skal opfylde de betingelser, der er omhandlet i GDPR, artikel 28, stk. 2, og stk. 4, for at gøre brug af en anden databehandler (en underdatabehandler).
- 7.2 Databehandleren må således ikke gøre brug af en underdatabehandler til opfyldelse af disse Bestemmelser uden forudgående generel skriftlig godkendelse fra den Dataansvarlige.
- 7.3 Databehandleren har den Dataansvarliges generelle godkendelse til brug af underdatabehandlere. Databehandleren skal skriftligt underrette den Dataansvarlige

om eventuelle planlagte ændringer vedrørende tilføjelse eller udskiftning af underdatabehandlere med mindst 30 kalenderdages varsel og derved give den Dataansvarlige mulighed for at gøre indsigelse mod sådanne ændringer inden brugen af de(n) omhandlede underdatabehandler(e). Længere varsel for underretning i forbindelse med specifikke behandlingsaktiviteter kan angives i Bilag B. Listen over underdatabehandlere, som den Dataansvarlige allerede har godkendt, fremgår af Bilag B.

- 7.4 Når Databehandleren gør brug af en underdatabehandler i forbindelse med udførelse af specifikke behandlingsaktiviteter på vegne af den Dataansvarlige, skal Databehandleren, gennem en kontrakt eller andet retligt dokument i henhold til EU-retten eller EU-/EØS-medlemsstaternes nationale ret, pålægge underdatabehandleren de samme databeskyttelsesforpligtelser som dem, der fremgår af disse Bestemmelser, hvorved der navnlig stilles de fornødne garantier for, at underdatabehandleren vil gennemføre de tekniske og organisatoriske foranstaltninger på en sådan måde, at behandlingen overholder kravene i disse Bestemmelser og GDPR.

Databehandleren er derfor ansvarlig for at kræve, at underdatabehandleren som minimum overholder Databehandlerens forpligtelser efter disse Bestemmelser og GDPR.

- 7.5 Underdatabehandleraftale(r) og eventuelle senere ændringer hertil sendes – efter den Dataansvarliges anmodning herom – i kopi til den Dataansvarlige, som herigennem har mulighed for at sikre sig, at tilsvarende databeskyttelsesforpligtelser som følger af disse Bestemmelser er pålagt underdatabehandleren. Bestemmelser om kommercielle vilkår, som ikke påvirker det databeskyttelsesretlige indhold af underdatabehandleraftalen, skal ikke sendes til den Dataansvarlige.
- 7.6 Databehandleren skal i sin aftale med underdatabehandleren indføre 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 underdatabehandlere, som f.eks. gør den Dataansvarlige i stand til at instruere underdatabehandleren i at slette eller tilbagelevere personoplysningerne.
- 7.7 Hvis underdatabehandleren ikke opfylder sine databeskyttelsesforpligtelser, forbliver Databehandleren fuldt ansvarlig over for den Dataansvarlige for opfyldelsen af underdatabehandlerens forpligtelser. Dette påvirker ikke de registreredes rettigheder, der følger af GDPR, herunder særligt GDPR, artikel 79 og 82, over for den Dataansvarlige og Databehandleren, herunder underdatabehandleren.

8. **Overførsel til tredjelande eller internationale organisationer**

- 8.1 Enhver overførsel af personoplysninger til tredjelande eller internationale organisationer må kun foretages af Databehandleren på baggrund af dokumenteret instruks herom fra den Dataansvarlige og skal altid ske i overensstemmelse med GDPR, kapitel V.
- 8.2 Hvis overførsel af personoplysninger til tredjelande eller internationale organisationer, som Databehandleren ikke er blevet instrueret i at foretage af den Dataansvarlige,

kræves i henhold til EU-ret eller EU-/EØS-medlemsstaternes nationale ret, som Databehandleren er underlagt, skal Databehandleren underrette den Dataansvarlige om dette retlige krav inden behandling, medmindre den pågældende ret forbyder en sådan underretning af hensyn til vigtige samfundsmæssige interesser.

- 8.3 Uden dokumenteret instruks fra den Dataansvarlige kan Databehandleren således ikke inden for rammerne af disse Bestemmelser:
- 8.3.1 overføre personoplysninger til en dataansvarlig eller databehandler i et tredjeland eller en international organisation
 - 8.3.2 overlade behandling af personoplysninger til en underdatabehandler i et tredjeland
 - 8.3.3 behandle personoplysningerne i et tredjeland
- 8.4 Den dataansvarliges instruks vedrørende overførsel af personoplysninger til et tredjeland, herunder det eventuelle overførselsgrundlag i databeskyttelsesforordningens kapitel V, som overførslen er baseret på, skal angives i bilag C.6.
- 8.5 Disse Bestemmelser skal ikke forveksles med standardkontraktbestemmelser som omhandlet i GDPR, artikel 46, stk. 2, litra c og d, og disse Bestemmelser kan ikke udgøre et grundlag for overførsel af personoplysninger som omhandlet i GDPR, kapitel V, medmindre sådanne standardkontraktbestemmelser er vedhæftet i Bilag E.

9. **Bistand til den Dataansvarlige**

- 9.1 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 GDPR, kapitel III.

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

- 9.1.1 oplysningspligten ved indsamling af personoplysninger hos den registrerede
- 9.1.2 oplysningspligten, hvis personoplysninger ikke er indsamlet hos den registrerede
- 9.1.3 indsigtsretten
- 9.1.4 retten til berigtigelse
- 9.1.5 retten til sletning ("retten til at blive glemt")
- 9.1.6 retten til begrænsning af behandling
- 9.1.7 underretningspligten i forbindelse med berigtigelse eller sletning af

personoplysninger eller begrænsning af behandling

- 9.1.8 retten til dataportabilitet
 - 9.1.9 retten til indsigelse
 - 9.1.10 retten til ikke at være genstand for en afgørelse, der alene er baseret på automatisk behandling, herunder profilering
- 9.2 I tillæg til Databehandlerens forpligtelse til at bistå den Dataansvarlige i henhold til bestemmelse 6.3, bistår Databehandleren endvidere, under hensyntagen til behandlingens karakter og de oplysninger, der er tilgængelige for Databehandleren, den Dataansvarlige med:
- 9.2.1 den Dataansvarliges forpligtelse til uden unødigt forsinkelse og om muligt senest 72 timer, efter at denne er blevet bekendt med det, at anmelde brud på persondatasikkerheden til Datatilsynet eller en anden kompetent tilsynsmyndighed, som måtte have kompetence, medmindre at det er usandsynligt, at bruddet på persondatasikkerheden indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder
 - 9.2.2 den Dataansvarliges forpligtelse til uden unødigt forsinkelse at underrette den registrerede om brud på persondatasikkerheden, når bruddet sandsynligvis vil medføre en høj risiko for fysiske personers rettigheder og frihedsrettigheder
 - 9.2.3 den Dataansvarliges forpligtelse til forud for behandlingen at foretage en analyse af de påtænkte behandlingsaktiviteters konsekvenser for beskyttelse af personoplysninger (en konsekvensanalyse)
 - 9.2.4 den Dataansvarliges forpligtelse til at høre Datatilsynet eller en anden kompetent tilsynsmyndighed, som måtte have kompetence 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.
- 9.3 Parterne skal i Bilag C angive de fornødne tekniske og organisatoriske foranstaltninger, hvormed Databehandleren skal bistå den Dataansvarlige samt i hvilket omfang og udstrækning. Det gælder for de forpligtelser, der følger af Bestemmelse 9.1 og 9.2.

10. **Underretning om brud på persondatasikkerheden**

- 10.1 Databehandleren underretter uden unødigt forsinkelse den Dataansvarlige efter at være blevet opmærksom på, at der er sket et brud på persondatasikkerheden.
- 10.2 Databehandlerens underretning til den Dataansvarlige skal om muligt ske straks og senest 12 timer efter det tidspunkt, hvor Databehandleren er blevet bekendt med bruddet på persondatasikkerheden, at denne er blevet bekendt med bruddet, sådan at den Dataansvarlige kan overholde sin forpligtelse til at anmelde bruddet på

persondatasikkerheden til den kompetente tilsynsmyndighed, jf. GDPR, artikel 33.

10.3 I overensstemmelse med bestemmelse 9.2.1 skal Databehandleren bistå den Dataansvarlige med at foretage anmeldelse af bruddet til den kompetente tilsynsmyndighed. Det betyder, at Databehandleren skal bistå med at tilvejebringe nedenstående information, som ifølge artikel 33, stk. 3, skal fremgå af den Dataansvarliges anmeldelse af bruddet til den kompetente tilsynsmyndighed:

10.3.1 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

10.3.2 de sandsynlige konsekvenser af bruddet på persondatasikkerheden

10.3.3 de foranstaltninger, som den Dataansvarlige har truffet eller foreslår truffet for at håndtere bruddet på persondatasikkerheden, herunder, hvis det er relevant, foranstaltninger for at begrænse dets mulige skadevirkninger.

10.4 Parterne skal i Bilag C angive den information, som Databehandleren skal tilvejebringe i forbindelse med sin bistand til den Dataansvarlige i dennes forpligtelse til at anmelde brud på persondatasikkerheden til den kompetente tilsynsmyndighed.

11. **Sletning og returnering af oplysninger**

11.1 Ved ophør af tjenesterne vedrørende behandling af personoplysninger, er Databehandleren forpligtet til at tilbagelevere alle personoplysningerne og slette eksisterende kopier, medmindre EU-retten eller EU-/EØS-medlemsstaternes nationale ret foreskriver opbevaring af personoplysningerne.

12. **Revision, herunder inspektion**

12.1 Databehandleren stiller alle oplysninger, der er nødvendige for at påvise overholdelsen af GDPR, artikel 28, og disse Bestemmelser, til rådighed for den Dataansvarlige og giver mulighed for og bidrager til revisioner, herunder inspektioner, der foretages af den Dataansvarlige eller en anden revisor, som er bemyndiget af den Dataansvarlige.

12.2 Procedurerne for den Dataansvarliges revisioner, herunder inspektioner, med Databehandleren og underdatabehandlere er nærmere angivet i Bilag C.7 og C.8 .

12.3 Databehandleren er forpligtet til at give tilsynsmyndigheder, som efter gældende lovgivning har adgang til den Dataansvarliges eller Databehandlerens faciliteter, eller repræsentanter, der optræder på tilsynsmyndighedens vegne, adgang til Databehandlerens fysiske faciliteter mod behørig legitimation.

13. **Parternes aftale om andre forhold**

- 13.1 Parterne kan aftale andre bestemmelser vedrørende tjenesten vedrørende behandling af personoplysninger om f.eks. erstatningsansvar, så længe disse andre bestemmelser ikke direkte eller indirekte strider imod Bestemmelserne eller forringer den registreredes grundlæggende rettigheder og frihedsrettigheder, som følger af GDPR.

14. **Ikrafttræden og ophør**

- 14.1 Bestemmelserne er bindende mellem Parterne.
- 14.2 Begge Parter kan kræve Bestemmelserne genforhandlet, hvis lovændringer eller uhensigtsmæssigheder i Bestemmelserne giver anledning hertil.
- 14.3 Bestemmelserne er gældende, så længe tjenesten vedrørende behandling af personoplysninger varer. I denne periode kan Bestemmelserne ikke opsiges, medmindre andre bestemmelser, der regulerer levering af tjenesten vedrørende behandling af personoplysninger, aftales mellem Parterne.
- 14.4 Hvis levering af tjenesterne vedrørende behandling af personoplysninger ophører, og personoplysningerne er slettet eller returneret til den Dataansvarlige i overensstemmelse med Bestemmelse 11.1 og Bilag C.4, kan Bestemmelserne opsiges med skriftlig varsel af begge Parter.
- 14.5 Databehandleren er bundet af Bestemmelserne uden Parternes underskrift. Bestemmelserne indgås således uden fysiske/digitale underskrifter, idet Bestemmelserne er bindende i overensstemmelse med kravet i GDPR, artikel 28, stk. 3, 1. pkt.

15. **Kontaktpersoner hos den Dataansvarlige og Databehandleren**

- 15.1 Parterne kan kontakte hinanden via nedenstående kontaktpersoner.
- 15.2 Parterne er forpligtet til løbende at orientere hinanden om ændringer vedrørende kontaktpersoner.

Kontaktoplysninger for den Dataansvarlige:

Kontaktoplysninger for Databehandleren:

Niels Arnold Lund, NAL@board-office.dk

Bilag A Oplysninger om behandlingen

1. **Formålet med Databehandlerens behandling af personoplysninger på vegne af den Dataansvarlige**

1.1 Følgende formål ligger til grund for Databehandlerens behandling af personoplysninger på vegne af den Dataansvarlige:

Den dataansvarlige ønsker at anvende Databehandlerens bestyrelsesportal BOARD-OFFICE, som er en online portal, som indeholder dokumentlager, debatforum, et planlægningsværktøj, digital signatur, opslag af bestyrelsesjobs samt inspirationsområde.

Herudover forestår Databehandleren drift, test, vedligeholdelse, udvikling samt fejlretning af Databehandlerens applikationer.

2. **Databehandlerens behandling af personoplysninger på vegne af den Dataansvarlige drejer sig primært om (karakteren af behandlingen)**

2.1 Databehandleren behandler Personoplysningerne i forbindelse med Databehandlerens levering af bestyrelsesportalen BOARD-OFFICE & BOARD-PEOPLE.

3. **Behandlingen omfatter følgende typer af personoplysninger om de registrerede**

3.1 navn, adresse, telefonnummer, e-mail, brugernavn til et eller flere systemer, adgangskode til et eller flere systemer, varierende personoplysninger, som kunden eller kundens kunder afgiver eller registrerer uden organisationens aktive behandling og identificering heraf

3.2 Databehandleren behandler muligvis personoplysninger om den Dataansvarliges medarbejdere i forbindelse med Databehandlerens salg, markedsføring og produktudvikling. Disse personoplysninger er ikke omfattet af Bestemmelserne, fordi Databehandleren er dataansvarlig for disse personoplysninger, og der henvises i stedet til Databehandlerens persondatapolitik, som kan findes på Databehandlerens hjemmeside eller efter anmodning.

4. **Behandlingen omfatter følgende kategorier af registrerede**

4.1 Ledelse og bestyrelsesmedlemmer.

5. **Databehandlerens behandling af personoplysninger på vegne af den Dataansvarlige kan påbegyndes efter disse Bestemmelers ikrafttræden. Behandlingen har følgende varighed**
- 5.1 Personoplysningerne behandles indtil ophør af tjenesterne vedrørende behandling af personoplysninger, hvorefter personoplysningerne slettes eller returneres i overensstemmelse med afsnit 11. Behandlingen foretages således så længe den eller de bagvedliggende kommercielle aftaler består.

Bilag B Underdatabehandlere

1. **Godkendte underdatabehandlere**

- 1.1 Ved Bestemmelsernes ikrafttræden har den Dataansvarlige godkendt brugen af følgende underdatabehandlere:

Databehandlerens underdatabehandlere er oplistet i den til enhver tid gældende liste over underdatabehandlere, der kan tilgås under 'Sikkerhed' fanen på vores hjemmeside, eller under 'Indstillinger' inde på de individuelle portaler.

- 1.2 Ved Bestemmelsernes ikrafttræden har den Dataansvarlige godkendt brugen af ovennævnte underdatabehandlere for den beskrevne behandlingsaktivitet. Databehandleren må ikke – uden den Dataansvarliges skriftlige godkendelse – gøre brug af en underdatabehandler til en anden behandlingsaktivitet end den beskrevne og aftalte eller gøre brug af en anden underdatabehandler til denne behandlingsaktivitet.

Bilag C Instruks vedrørende behandling af personoplysninger

1. Behandlingens genstand/instruks

- 1.1 Databehandleren behandler personoplysninger på vegne af den Dataansvarlige med henblik på at gøre den Dataansvarlige i stand til at anvende bestyrelsesportalen BOARD-OFFICE & BOARD-PEOPLE, som er en online portal, der indeholder dokumentlager, debatforum, et planlægningsværktøj, digital signatur, opslag af bestyrelsesjobs samt inspirationsområde.

2. Behandlingssikkerhed

- 2.1 Sikkerhedsniveauet skal afspejle:

Databehandleren skal etablere et passende sikkerhedsniveau under hensyntagen til behandlingens karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder.

Databehandleren er herefter berettiget og forpligtet til at træffe beslutninger om, hvilke tekniske og organisatoriske sikkerhedsforanstaltninger, der skal gennemføres for at etablere det nødvendige (og aftalte) sikkerhedsniveau.

Databehandleren skal dog - under alle omstændigheder og som minimum - gennemføre følgende foranstaltninger, som er aftalt med den Dataansvarlige:

Fysisk sikkerhed

Databehandleren gennemfører følgende fysiske sikkerhedsforanstaltninger:

- a) Databehandlerens kontorlokaler kan aflåses.
- b) Databehandleren har alarmsystem til at opdage og forhindre indbrud.
- c) Databehandleren har brandalarm og røgdetektorer.
- d) Databehandleren udstyr (herunder PC'er, eventuelle servere mv.) er sikret bag låste døre.
- e) Der er overvågning af databehandlerens bygninger, lokaler og faciliteter eller adgangsveje (billede eller videoovervågning).
- f) Der anvendes kontrolproces eller -system til kontrol med besøgendes identitet.
- g) Databehandleren anvender nøglestyring, dvs. udlevere nøgler til de relevante og nødvendige medarbejdere mv.
- h) Der føres protokol over Databehandlerens besøgende.

Organisatorisk sikkerhed

Databehandleren gennemfører følgende foranstaltninger organisatoriske sikkerhedsforanstaltninger:

- a) Alle medarbejdere er underlagt fortrolighedsforpligtelse, der gælder for alle behandlede personoplysninger.
- b) Medarbejdernes adgang til personoplysninger i systemer og på eventuelle fysiske

- medier eller faciliteter er begrænset, sådan at det kun er de relevante medarbejdere, der har adgang til de relevante personoplysninger.
- c) Medarbejdere med adgang til personoplysninger eller kritiske it-systemer er sikkerhedsgodkendt forinden ansættelse
 - d) Medarbejderes behandling af personoplysninger logges helt eller delvis og kan kontrolleres efter behov.
 - e) Databehandleren har en dokumenteret procesbeskrivelse for brud på persondatasikkerheden, der minimum tages op til revidering årligt.
 - f) Databehandleren har en it-sikkerhedspolitik.
 - g) Databehandleren har en fast proces, der sikrer, at der ved reparation, service og kassation af hardware sørges for sletning eller fortsat fortrolighed vedrørende personoplysninger på det berørte hardware.

Teknisk sikkerhed: Adgang til og beskyttelse af systemer

Databehandleren gennemfører følgende tekniske sikkerhedsforanstaltninger vedrørende adgang til og beskyttelse af systemer:

- a) Databehandlerens systemer har logisk adgangskontrol ved brugernavn og adgangskode eller anden autorisation.
- b) Databehandlerens kræver, at medarbejdere anvender individuelle adgangskoder (passwords).
- c) Databehandlerens PC'er har automatisk adgangsbeskyttelse ved inaktivitet, dvs. låst pauseskærm.
- d) Databehandlerens benytter antivirus-programmer, som opdateres jævnligt.
- e) Der anvendes politik for sammensætningen af adgangskoder, herunder minimumskrav.
- f) Der er procedure(r) for tilbagekaldelse af tilladelser, når en medarbejder stopper hos Databehandleren eller skifter afdeling.
- g) Der foretages logning og kontrol af uautoriserede eller gentagne mislykkede forsøg på log-in på Databehandlerens systemer.

Automatisk daglig backup af databasen, gennem storage- og backupløsningen IBM Tivoli Storage Manager.

Personoplysninger krypteres i systemer og/eller på opbevaringsmedier, hvor det er relevant og under hensyntagen til behandlingen og personoplysningernes karakter.

Firewall, som opdateres kontinuerligt i henhold til at kunne bevare en fuldstændig beskyttelse.

Antivirus programmer, som opdateres kontinuerligt i henhold til at sikre, at både programmets moduler og systemkomponenter kan bevare en fuldstændig beskyttelse.

Databehandlerens websites anvender HTTPS (Hyper Text Transfer Protocol Secure), så alt kommunikation på det åbne internet er krypteret peer-to-peer.

Teknisk sikkerhed: Adgang til personoplysninger (data)

Databehandleren gennemfører følgende tekniske sikkerhedsforanstaltninger vedrørende adgang til personoplysninger:

- a) Databehandleren foretager regelmæssig gennemgang og kontrol af brugerautorisationer til specifikke systemer.
- b) Databehandleren har sporbarhed af adgang til, ændring af og sletning af data foretaget af individuelle brugere.
- c) Databehandleren tildeler enkelte eller grupper af brugere autorisationer til at tilgå, ændre og slette behandlede personoplysninger.
- d) Databehandleren har procedure(r) for at genskabe/retablere data fra backup.

Teknisk sikkerhed: Kryptering

Databehandleren gennemfører følgende tekniske sikkerhedsforanstaltninger vedrørende kryptering:

- a) Indhold på eksterne harddiske og USB-nøgler mv. er krypteret, når disse medier indeholder personoplysninger eller følsomme personoplysninger.
- b) Databehandlerens hjemmesider anvender HTTPS (Hyper Text Transfer Protocol Secure).
- c) Databehandlerens computere har krypterede harddiske.
- d) Personoplysninger krypteres i relevante systemer og/eller på opbevaringsmedier.
- e) Adgangskoder opbevaret på databehandlerens computere mv. er krypterede.
- f) Følsomme personoplysninger krypteres i systemer og/eller på opbevaringsmedier.

Teknisk sikkerhed: Kontrol af transmission

Databehandleren gennemfører følgende tekniske sikkerhedsforanstaltninger vedrørende kontrol af transmission:

- a) Databehandleren anvender og har retningslinjer for sikker e-mail.
- b) Udgående e-mails med følsomme personoplysninger eller oplysninger om rent private forhold krypteres.
- c) Retningslinjer for brug af arbejdsmail, herunder brug til privat brug, passende brug, kryptering, sikker brug mv.

Teknisk sikkerhed: Tilgængelighed og robusthed

Databehandleren gennemfører følgende tekniske sikkerhedsforanstaltninger vedrørende tilgængelighed og robusthed:

- a) Tilgængelighed og robusthed i Databehandlerens systemer og servere er sikret af tredjemand, som Databehandleren har en aftale med.
- b) Kun autoriserede medarbejdere har adgang til Databehandlerens eventuelle egne servere.
- c) Serverrum har røgalarm og brandslukkere.

- d) Serverrum har airconditionssystem.
- e) Der er regler og retningslinjer for backup af data.
- f) Der er regler og retningslinjer for genskabelse af data fra backup.
- g) Der foretages regelmæssig backup (enten egen eller hos leverandør).
- h) Aktiv alarmering ved forsøg på uautoriseret adgang til serverrum og/eller behandlingssystemer og data.
- i) Der anvendes uafbrudt strømforsyning (UPS).
- j) Temperatur og luftfugtighed overvåges i serverrum.
- k) Databehandlerens har procedurebeskrivelse(r) for brud på persondatasikkerheden, der minimum tages op til revidering årligt.

3. **Bistand til den dataansvarlige**

3.1 Databehandleren skal så vidt muligt – inden for det nedenstående omfang og udstrækning – bistå den Dataansvarlige i overensstemmelse med Bestemmelse 9.1 og 9.2 ved at gennemføre følgende tekniske og organisatoriske foranstaltninger:

3.1.1 Hvis den Dataansvarlige modtager en anmodning om udøvelsen af personers rettigheder efter gældende databeskyttelseslovgivning, og korrekt besvarelse af anmodningen kræver bistand fra Databehandleren, skal Databehandleren bistå den Dataansvarlige med nødvendige og relevante oplysninger og dokumentation samt passende tekniske og organisatoriske sikkerhedsforanstaltninger.

3.1.2 Hvis den Dataansvarlige vil have hjælp til at besvare en anmodning fra en registreret person, skal den Dataansvarlige sende skriftlig anmodning herom til Databehandleren, og Databehandleren skal som svar herpå levere den nødvendige hjælp eller dokumentation hurtigst muligt og senest 7 kalenderdage efter modtagelse af anmodning herom.

3.1.3 Hvis Databehandleren modtager en anmodning om udøvelsen af personers rettigheder efter gældende databeskyttelseslovgivning fra andre end den Dataansvarlige, og anmodningen vedrører personoplysninger behandlet på vegne af den Dataansvarlige, skal Databehandleren uden unødvendig forsinkelse videresende anmodningen til den Dataansvarlige.

4. **Opbevaringsperiode/sletterutine**

4.1 Ved ophør af tjenesten vedrørende behandling af personoplysninger, skal Databehandleren enten slette eller tilbagelevere personoplysningerne i overensstemmelse med Bestemmelse 11.1 medmindre den Dataansvarlige – efter underskriften af disse bestemmelser – har ændret sit oprindelige valg. Sådanne ændringer skal være dokumenteret og opbevares skriftligt, herunder elektronisk, i tilknytning til Bestemmelserne.

5. **Lokalitet for behandling**

- 5.1 Behandling af de af Bestemmelserne omfattede personoplysninger kan ikke uden den Dataansvarliges forudgående skriftlige godkendelse ske på andre lokaliteter end følgende:

Hos Databehandleren egne hovedkontorer og på hovedkontorerne for godkendte underdatabehandlere, som angivet i bilag B.

6. **Instruks vedrørende overførsel af personoplysninger til tredjelande**

- 6.1 Personoplysningerne behandles kun af Databehandleren på de lokationer, som er beskrevet i Bestemmelse C.5. Databehandleren overfører ikke personoplysninger til tredjelande eller internationale organisationer.
- 6.2 I det omfang personoplysninger overføres til tredjelande, som ikke har været genstand for en afgørelse om tilstrækkelig sikkerhed efter GDPR, artikel 45, hvor begge parter er dataansvarlige, og denne overførsel ikke er omfattet af en eller flere af undtagelsesreglerne i artikel 49, skal retsgrundlaget ligeledes være standardkontraktbestemmelser som indeholdt i bilag E.
- 6.3 Hvis den Dataansvarlige ikke i disse Bestemmelser eller efterfølgende giver en dokumenteret instruks vedrørende overførsel af personoplysninger til et tredjeland, er Databehandleren ikke berettiget til inden for rammerne af disse Bestemmelser at foretage sådanne overførsler.
- 6.4 Overførsel af personoplysninger må i alle tilfælde kun ske som foreskrevet i Bestemmelserne, på den Dataansvarliges instruks, og i det omfang det er tilladt i medfør af databeskyttelseslovgivningen.
- 6.5 Såfremt overførslen af personoplysningerne til tredjelande udenfor EU/EØS sker ved Databehandlerens overførsel til underdatabehandlere, giver den Dataansvarlige ved Bestemmelserne fuldmagt til, at Databehandleren på vegne af den Dataansvarlige kan indgå standardkontraktbestemmelserne vedtaget af Kommissionen med Databehandlerens underdatabehandlere, forudsat at alle regler i databeskyttelseslovgivningen for overførsel og behandling i øvrigt efterleves. Såfremt den Dataansvarlige selv er databehandler, og Databehandleren optræder som underdatabehandler for personoplysningerne i forhold til den Dataansvarliges ultimative kontraktpart(er), skal den Dataansvarlige indhente fuldmagt fra den ultimative kontraktpart til Databehandlerens indgåelse af standardkontraktbestemmelserne.
- 6.6 Når Databehandleren, i overensstemmelse med disse bestemmelser, overfører personoplysninger omfattet af aftalen videre til underdatabehandlere eller selvstændigt dataansvarlige i tredjelande, skal Databehandleren selv sørge for at sikre, at overførslen overholder kapitel 5 i Forordning 2016/679.

7. Procedurer for den Dataansvarliges revisioner, herunder inspektioner, med behandlingen af personoplysninger, som er overladt til Databehandleren

7.1 Databehandleren skal på skriftlig anmodning dokumentere overfor den Dataansvarlige, at Databehandleren

7.1.1 overholder sine forpligtelser efter denne Databehandleraftale og Instruksen, og

7.1.2 overholder bestemmelserne i GDPR, for så vidt angår personoplysningerne, som behandles på den Dataansvarliges vegne.

7.2 Databehandlerens dokumentation i henhold til afsnit C.7.1 skal sendes til den Dataansvarlige inden for rimelig tid efter modtagelsen af anmodningen herom.

7.3 Databehandleren skal som dokumentation for løbende overholdelse af Bestemmelserne stille egenkontrolrapporter til rådighed for den Dataansvarlige. Disse egenkontrolrapporter skal som minimum udarbejdes én gang årligt og skal følge principperne og kontrolmålene i revisionsstandarden ISAE 3000 som udarbejdet af FSR-danske revisorer og Datatilsynet (og/eller alternativt andre internationalt anerkendte standarder såsom ISO/IEC 27701:2019). Egenkontrolrapporterne kan efter den Dataansvarliges valg ske ved den Dataansvarliges informationsindsamling og skal underskrives af Databehandlerens ledelse. Databehandleren er ikke forpligtet til selv at iværksætte og gennemføre ekstern revision (audit) af Databehandlerens overholdelse af Bestemmelserne.

7.4 Uanset afsnit C.7.3 skal Databehandleren derudover give mulighed for og bidrage til revisioner og inspektioner hver 12. måned, der foretages af revisorer udpeget af den Dataansvarlige, de offentlige myndigheder i Danmark eller af anden kompetent jurisdiktion, i det omfang det er nødvendigt for at kontrollere, at Databehandleren overholder Bestemmelserne og gældende databeskyttelseslovgivning. Den pågældende revisor skal være underlagt fortrolighed i henhold til lov eller aftale. Den Dataansvarlige skal skriftligt varsle revisioner som beskrevet med 10 kalenderdage.

8. Procedurer for revisioner, herunder inspektioner, med behandling af personoplysninger, som er overladt til underdatabehandlere

8.1 Databehandleren skal være ansvarlig for at føre tilsyn med anvendte underdatabehandlere ved at udføre egenkontrolrapporter efter principperne i ISAE 3000 standarden.

Den dataansvarlige vil blive gjort opmærksom på eventuelle ændringer der vurderes at have betydning og relevans for behandlingen af deres data.

Bilag D Parternes regulering af andre forhold