Databehandleraftale

Imellem:

Dataansvarlig
[Virksomhedens navn og kontaktperson – udfyldes ved indgåelse]
Kontaktperson: [E-mail]

og

Databehandler
Book aps
Njalsgade 76
2300 København S
Danmark
CVR: 43159666
Kontakt: info@book.dk

Indhold

1. Baggrund for databehandleraftalen
2. Den Dataansvarliges rettigheder og forpligtelser
3. Databehandleren handler efter instruktioner
4. Fortrolighed
5. Sikkerhed ved behandling
6. Brug af underdatabehandlere
7. Overførsler til tredjelande
8. Bistand til den Dataansvarlige
9. Brud på persondata
10. Sletning og returnering af data
11. Adgang og revision
12. Ansvar

13. Ikrafttræden og ophør
14. Meddelelser
15. Gældende lov og værneting
Bilag A – Oplysninger om behandlingen
Bilag B – Underdatabehandlere
Bilag C – Informationssikkerhed

1. Baggrund for databehandleraftalen

1.1. Denne databehandleraftale ("Databehandleraftalen") fastsætter de rettigheder og forpligtelser, der gælder for behandling af personoplysninger af Databehandleren, der handler på vegne af den Dataansvarlige.

1.2. Formålet med denne Databehandleraftale er at sikre, at parterne overholder 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 ("den generelle forordning om databeskyttelse" eller "GDPR") og gældende dansk lov, der implementerer den generelle forordning om databeskyttelse (herefter samlet benævnt "databeskyttelseslovgivningen").

1.3. Databehandlerens behandling af personoplysninger udføres med henblik på at opfylde hovedaftalen mellem parterne: "Vilkår og betingelser" ("Hovedaftalen"). Behandlingen er beskrevet mere detaljeret i Bilag A (Oplysninger om behandlingen).

1.4. I denne Databehandleraftale skal "personoplysninger", "Dataansvarlig", "Databehandler", "registreret", "behandling", "brud på persondatasikkerheden", "tilsynsmyndighed" og "tredjelande" forstås i overensstemmelse med databeskyttelseslovgivningen.

1.5. I tilfælde af uoverensstemmelse mellem denne Databehandleraftale og Hovedaftalen har Databehandleraftalen forrang i alle forhold vedrørende Databehandlerens behandling af personoplysninger på vegne af den Dataansvarlige.

1.6. Denne Databehandleraftale består af denne hoveddel af aftalen og følgende bilag: Bilag A (Oplysninger om behandlingen), Bilag B (Underdatabehandlere) og Bilag C (Informationssikkerhed).

1.7. Databehandleraftalen og tilhørende dokumenter opbevares i et skriftligt elektronisk format af begge parter.

1.8. Denne Databehandleraftale fritager ikke Databehandleren for forpligtelser, der direkte pålægges Databehandleren i henhold til databeskyttelseslovgivningen.

2. Den Dataansvarliges rettigheder og forpligtelser

2.1. Den Dataansvarlige er ansvarlig for at sikre, at behandlingen af personoplysninger sker i overensstemmelse med databeskyttelseslovgivningen.

2.2. Den Dataansvarlige har ret og pligt til at fastsætte formålet med behandlingen af personoplysninger og de midler, der skal anvendes.

2.3. Den Dataansvarlige er blandt andet ansvarlig for at sikre, at den behandling, som den instruerer Databehandleren om at udføre, er understøttet af et lovligt grundlag.

3. Databehandleren handler efter instruktioner

3.1. Databehandleren må kun behandle personoplysninger i overensstemmelse med dokumenterede instruktioner fra den Dataansvarlige, medmindre Databehandleren er forpligtet i henhold til EU/EØS-retten eller en medlemsstats ret til at behandle personoplysninger på en anden måde. Hvis en sådan retlig forpligtelse opstår, skal Databehandleren underrette den Dataansvarlige om det retlige krav inden behandlingen, medmindre loven forbyder en sådan underretning, jf. GDPR artikel 28(3)(a).

3.2. Databehandleren skal straks underrette den Dataansvarlige, hvis Databehandleren mener, at en instruktion fra den Dataansvarlige overtræder databeskyttelseslovgivningen.

4. Fortrolighed

4.1. Databehandleren skal sikre, at adgangen til de personoplysninger, der behandles på den Dataansvarliges vegne, er begrænset til personer, der er bemyndiget til at have sådan adgang.

4.2. Databehandleren skal sikre, at de personer, der er bemyndiget til at behandle personoplysninger på den Dataansvarliges vegne, er underlagt en lovbestemt eller kontraktlig tavshedspligt.

4.3. Efter anmodning fra den Dataansvarlige skal Databehandleren kunne påvise, at ansatte og andre personer, der er bemyndiget til at behandle personoplysninger, er underlagt en tavshedspligt.

5. Sikkerhed ved behandling

5.1. Databehandleren skal implementere passende tekniske og organisatoriske foranstaltninger i henhold til artikel 32 i GDPR for at sikre et tilstrækkeligt sikkerhedsniveau.

5.2. Ovenstående forpligtelse indebærer risikovurdering og foranstaltninger til at håndtere identificerede risici, herunder: pseudonymisering og kryptering; fortrolighed, integritet,

tilgængelighed og robusthed; rettidig genoprettelse; og regelmæssig testning og vurdering af foranstaltningernes effektivitet.

5.3. De relevante foranstaltninger er specificeret i Bilag C. Den Dataansvarlige skal give Databehandleren alle nødvendige oplysninger til at identificere og vurdere risici.

6. Brug af underdatabehandlere

6.1. Databehandleren skal overholde betingelserne i artikel 28(2) og (4) i GDPR for at kunne engagere underdatabehandlere.

6.2. Databehandleren må ikke anvende en underdatabehandler uden den Dataansvarliges forudgående skriftlige samtykke.

6.3. Den Dataansvarlige giver hermed Databehandleren sin generelle tilladelse til at anvende underdatabehandlere til at opfylde Databehandleraftalen. Underdatabehandlere er angivet i Bilag B.

6.4. Ved udskiftning eller udpegelse af nye underdatabehandlere skal Databehandleren underrette den Dataansvarlige inden for rimelig tid, inden den nye underdatabehandler anvendes. Den Dataansvarlige kan gøre indsigelse mod ændringer. Hvis den Dataansvarlige gør indsigelse, skal parterne i god tro indlede drøftelser for at finde en løsning.

6.5. Databehandleren skal sikre, at underdatabehandlere er bundet af de samme forpligtelser som dem, der påhviler Databehandleren i henhold til denne aftale.

6.6. Databehandlerens brug af underdatabehandlere skal ikke reducere eller begrænse Databehandlerens ansvar og forpligtelser i henhold til denne Databehandleraftale.

7. Overførsler til tredjelande eller internationale organisationer

7.1. Databehandleren må ikke uden den Dataansvarliges forudgående skriftlige samtykke overføre eller på anden måde foranledige, at personoplysninger overføres uden for EU/EØS-området til tredjelande eller internationale organisationer, der ikke sikrer et tilstrækkeligt beskyttelsesniveau. Før samtykke gives, kan den Dataansvarlige kræve passende sikkerhedsforanstaltninger, herunder EU-Kommissionens standardkontraktbestemmelser.

8. Bistand til den Dataansvarlige

8.1. Databehandleren skal bistå den Dataansvarlige med at besvare anmodninger fra registrerede vedrørende udøvelsen af deres rettigheder i henhold til kapitel III i GDPR.

8.2. Under hensyntagen til behandlingens art skal Databehandleren bistå den Dataansvarlige med at sikre overholdelse af forpligtelserne i artikel 32-36 i GDPR, herunder forpligtelsen til DPIA og konsultation af Datatilsynet ved høj risiko.

9. Brud på persondata

9.1. Databehandleren skal underrette den Dataansvarlige uden unødig forsinkelse efter at være blevet opmærksom på et brud på persondatasikkerheden hos Databehandleren eller en underdatabehandler. Databehandleren skal yde de nødvendige oplysninger og bistand, så den Dataansvarlige kan opfylde sine underretningsforpligtelser. Databehandleren skal træffe alle nødvendige foranstaltninger for at begrænse virkningen af bruddet.

10. Sletning og returnering af data

10.1. Ved ophør af Databehandleraftalen kan den Dataansvarlige instruere Databehandleren om at returnere alle personoplysninger til den Dataansvarlige eller til en tredjepart udpeget af den Dataansvarlige, eller anmode om sletning. Databehandleren skal inden for rimelig tid sende skriftlig bekræftelse på, at personoplysningerne er returneret og/eller slettet.

11. Adgang og revision

11.1. Databehandleren skal stille alle nødvendige oplysninger til rådighed for den Dataansvarlige for at påvise overholdelse af artikel 28 i GDPR og denne Databehandleraftale. Databehandleren skal muliggøre og bidrage til revisioner og inspektioner udført af den Dataansvarlige eller en bemyndiget revisor.

11.2. Den detaljerede procedure for den Dataansvarliges tilsyn med Databehandleren er beskrevet i Bilag C.

11.3. Den Dataansvarliges tilsyn med eventuelle underdatabehandlere udføres via Databehandleren.

12. Ansvar

12.1. Ansvarsbegrænsningen anført i Hovedaftalen gælder ligeledes for enhver misligholdelse af denne Databehandleraftale.

12.2. Parternes ansvar for tab, som registrerede eller andre fysiske personer lider som følge af overtrædelser af databeskyttelseslovgivningen, er underlagt artikel 82 i GDPR, uden at ovenstående begrænsning er omfattet af dette.

13. Ikrafttræden og ophør

13.1. Denne Databehandleraftale træder i kraft på datoen for begge parters underskrift eller ved den Dataansvarliges accept ved tilmelding til book.dk-platformen.

13.2. Hver part kan anmode om genforhandling af Databehandleraftalen, hvis ændringer i lovgivningen eller mangler giver grundlag herfor.

13.3. Eventuelle ændringer vedrørende aflønning, vilkår eller lignende vil være angivet i Hovedaftalen eller Bilag C.

13.4. Databehandleraftalen kan opsiges i overensstemmelse med bestemmelserne i Hovedaftalen.

13.5. Databehandleraftalen forbliver gældende, så længe Databehandleren behandler personoplysninger på vegne af den Dataansvarlige. Uanset ophør af Hovedaftalen forbliver Databehandleraftalen gældende, indtil behandlingen ophører og personoplysningerne slettes af Databehandleren og eventuelle involverede underdatabehandlere.

14. Meddelelser

14.1. Meddelelser skal sendes via e-mail som angivet i Bilag A.

15. Gældende lov og værneting

15.1. Bestemmelserne i Hovedaftalen om lovvalg og værneting finder tilsvarende anvendelse på denne Databehandleraftale.

Bilag A – Oplysninger om behandlingen

1. Formål med behandlingen

Databehandlerens behandling af personoplysninger på vegne af den Dataansvarlige sker med det formål at give adgang til og brug af book.dk-platformen, herunder:

- Klienthåndtering og kundeadministration
- Online booking af aftaler og hold/arrangementer
- Kalender- og tidsstyring
- Kommunikation mellem den Dataansvarlige og deres kunder (e-mail, SMS)
- Fakturering og betaling

- Journalføring (hvor aktiveret)

2. Behandlingens art

Behandlingen sker via book.dk-platformen og omfatter opbevaring og administration af klientdata, bookingoplysninger, kommunikation og faktureringsdata.

3. Behandlingens varighed

Behandlingen fortsætter, så længe Hovedaftalen mellem parterne er gældende, og indtil alle personoplysninger er slettet eller returneret i overensstemmelse med denne Databehandleraftale.

4. Kategorier af registrerede

- Den Dataansvarliges medarbejdere, der bruger platformen
- Den Dataansvarliges kunder/klienter, der booker aftaler eller interagerer via platformen

5. Typer af personoplysninger

- Navn
- E-mail
- Kontaktoplysninger (adresse, telefonnummer)
- CPR-nummer (hvor det er lovpligtigt, f.eks. sygeforsikring)
- Sundhedsdata (som særlig kategori, hvor journalføring er aktiveret)
- Bruger-ID tildelt af systemet
- Betalings-id'er og transaktionsdata

6. Særlige kategorier af data

Sundhedsdata i overensstemmelse med artikel 9 i GDPR (hvor journalføring eller sygeforsikring er aktiveret).

7. Brug af underdatabehandlere

Underdatabehandlere må kun anvendes til de formål, der er nødvendige for at levere de tjenester, der er beskrevet i dette Bilag A. Alle underdatabehandlere skal behandle data i overensstemmelse med den Dataansvarliges instruktioner og kun for at udføre deres udpegede funktioner.

Bilag B – Underdatabehandlere

Ved at indgå denne Databehandleraftale har den Dataansvarlige godkendt brugen af følgende underdatabehandlere:

Navn	Behandlingens art og formål	Kategorier af personoplysninger	Placering
DigitalOcean	Cloud hosting, databaser og servere	Alle personoplysninger	EU
Stripe	Behandling af online betalinger og abonnementer	Betalingskortoplysninger, faktureringsadresse, transaktionshistorik	USA og EU
SendGrid (Twilio)	E-mail	E-mailadresse og indhold af mailen	USA
Vipps MobilePay	MobilePay, kun når salonen har slået det til	Det, der skal til for betalingen. Pengene går til salonens konto	EØS
Zoom	Online møde, kun hvis en Zoom-konto er forbundet	Titel, tid, varighed og en kort beskrivelse	USA
Microsoft	Teams-møde, kun hvis en Microsoft 365-konto er forbundet	Titel, start, slut og en kort beskrivelse	EU og USA
GatewayAPI	SMS-beskedtjeneste	Telefonnumre, beskedindhold	Danmark
Google (reCAPTCHA)	Sikkerhedsvalidering (bot-detektion)	IP-adresse, brugerinteraktionsdata	USA
Google Calendar	Kalendersynkronisering (valgfrit)	Bookingdata, klientnavne (kun hvis aktiveret)	USA

Bemærk: Eventuelle nye underdatabehandlere vil blive underrettet den Dataansvarlige på forhånd. Underdatabehandlere må kun behandle data til de formål, der er beskrevet i Bilag A.

Bilag C – Informationssikkerhed

1. Sikkerhedsforanstaltninger

Databehandleren implementerer følgende tekniske og organisatoriske foranstaltninger i overensstemmelse med artikel 32 i GDPR:

- **Behandlingssikkerhed:** Sikker brugergodkendelse (f.eks. 2FA), rollebaserede adgangskontroller, TLS-kryptering undervejs, AES-256-kryptering i hvile
- **Risikovurdering:** Årlige risikovurderinger, løbende overvågning af risikoeksponering
- **HTTPS og certifikater:** Gyldige SSL-certifikater på alle tjenester
- **Brugeradgang:** Princippet om færrest rettigheder
- **Overvågning og logføring:** Systemaktivitetslogfiler med revisionsspor
- **Organisatoriske foranstaltninger:** Interne databeskyttelsespolitikker
- **Sikker kommunikation:** Krypterede kommunikationskanaler (HTTPS, TLS)
- **Kryptering:** Kryptering af personoplysninger både under transit og i lagring
- **Backup:** Daglig sikkerhedskopi i EU, som gemmes i 30 dage og kan genetableres på den Dataansvarliges anmodning

2. Instruktioner

Databehandleren må kun behandle personoplysninger baseret på dokumenterede instruktioner fra den Dataansvarlige som defineret i denne Databehandleraftale.

3. Opbevarings- og sletningsrutine

Data gemmes i aftalens løbetid. Ved ophør eller på den Dataansvarliges anmodning: Data slettes inden for 30 dage. Skriftlig bekræftelse på sletning gives. Sikre sletningsprocedurer anvendes på alle medier.

4. Behandlingens placering

Databaser og sikkerhedskopier ligger i EU/EØS. Overførsel til de underdatabehandlere i Bilag B, der står uden for EU/EØS, er godkendt med denne aftale og sker med EU-Kommissionens standardkontraktbestemmelser.

5. Revision og kontrol

Databehandleren foretager årlig intern revision af databehandlings- og informationssikkerhedskontroller. Resultaterne dokumenteres og er tilgængelige for den Dataansvarlige efter anmodning. Databehandleren tillader den Dataansvarlige at foretage revision eller udpege en tredjepart med rimeligt varsel.

6. Konkurs

I tilfælde af Databehandlerens konkurs skal den Dataansvarlige (eller udpeget tredjepart) have adgang til at hente personoplysninger og sikkerhedskopier for at sikre kontinuitet og beskyttelse af de registreredes rettigheder.

Book aps · Njalsgade 76 · 2300 København S · CVR: 43159666 · info@book.dk
Seneste opdatering: 05.11.2026