Senbee Databehandleraftale

Standardkontraktsbestemmelser

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

Mellem

Navn: _____

CVR: _____

Adresse:_____

herefter "den dataansvarlige"

og

Navn: Senbee A/S
CVR: 45638154
Adresse: Åbogade 15, 8200 Aarhus N

herefter "databehandleren"

der hver især er en "part" og sammen udgør "parterne"

HAR AFTALT følgende standardkontraktsbestemmelser (Bestemmelserne) med henblik på at overholde databeskyttelsesforordningen og sikre beskyttelse af privatlivets fred og fysiske personers grundlæggende rettigheder og frihedsrettigheder

1.Indhold

2.Præambel

1. Disse Bestemmelser fastsætter databehandlerens rettigheder og forpligtelser, når denne foretager behandling af personoplysninger på vegne af den dataansvarlige.

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 (databeskyttelsesforordningen).

3. I forbindelse med leveringen af Senbee Connect behandler databehandleren personoplysninger på vegne af den dataansvarlige i overensstemmelse med disse Bestemmelser.

4. Bestemmelserne har forrang i forhold til eventuelle tilsvarende bestemmelser i andre aftaler mellem parterne.

5. Der hører fire bilag til disse Bestemmelser, og bilagene udgør en integreret del af Bestemmelserne.

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.

7. Bilag B indeholder den dataansvarliges betingelser for databehandlerens brug af underdatabehandlere og en liste af underdatabehandlere, som den dataansvarlige har godkendt brugen af.

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.

9. Bestemmelserne med tilhørende bilag skal opbevares skriftligt, herunder elektronisk, af begge parter.

10. Disse Bestemmelser frigør ikke databehandleren fra forpligtelser, som databehandleren er pålagt efter databeskyttelsesforordningen eller enhver anden lovgivning.

3.Den dataansvarliges rettigheder og forpligtelser

1. Den dataansvarlige er ansvarlig for at sikre, at behandlingen af personoplysninger sker i overensstemmelse med databeskyttelsesforordningen (se forordningens artikel 24), databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse Bestemmelser.

2. Den dataansvarlige har ret og pligt til at træffe beslutninger om, til hvilke(t) formål og med hvilke hjælpemidler, der må ske behandling af personoplysninger.

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

1. Databehandleren må kun behandle personoplysninger efter dokumenteret instruks fra den dataansvarlige, medmindre det kræves i henhold til EU-ret eller medlemsstaternes nationale ret, som databehandleren er underlagt. 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.

2. Databehandleren underretter omgående den dataansvarlige, hvis en instruks efter vedkommendes mening er i strid med denne forordning eller databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret.

5.Fortrolighed

1. Databehandleren må kun give adgang til personoplysninger, som behandles på den dataansvarliges vegne, til personer, som er underlagt databehandlerens instruktionsbeføjelser, 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.

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

1. Databeskyttelsesforordningens 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:

   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.

2. Efter forordningens 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.

3. Derudover skal databehandleren bistå den dataansvarlige med vedkommendes overholdelse af den dataansvarliges forpligtelse efter forordningens 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 forordningens artikel 32, og al anden information, der er nødvendig for den dataansvarliges overholdelse af sin forpligtelse efter forordningens artikel 32.

4. 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

1. Databehandleren skal opfylde de betingelser, der er omhandlet i databeskyttelsesforordningens artikel 28, stk. 2, og stk. 4, for at gøre brug af en anden databehandler (en underdatabehandler).

2. Databehandleren må således ikke gøre brug af en underdatabehandler til opfyldelse af disse Bestemmelser uden forudgående generel skriftlig godkendelse fra den dataansvarlige.

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 dages 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.

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 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 databeskyttelsesforordningen.

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

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.

6. 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 databeskyttelsesforordningen, herunder særligt forordningens artikel 79 og 82, over for den dataansvarlige og databehandleren, herunder underdatabehandleren.

8.Overførsel til tredjelande eller internationale organisationer

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 databeskyttelsesforordningens kapitel V.

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 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.

3. Uden dokumenteret instruks fra den dataansvarlige kan databehandleren således ikke inden for rammerne af disse Bestemmelser:

    a. overføre personoplysninger til en dataansvarlig eller databehandler i et tredjeland eller en international organisation

    b. overlade behandling af personoplysninger til en underdatabehandler i et tredjeland

    c. behandle personoplysningerne i et tredjeland

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.

5. Disse Bestemmelser skal ikke forveksles med standardkontraktsbestemmelser som omhandlet i databeskyttelsesforordningens artikel 46, stk. 2, litra c og d, og disse Bestemmelser kan ikke udgøre et grundlag for overførsel af personoplysninger som omhandlet i databeskyttelsesforordningens kapitel V.

9.Bistand til den dataansvarlige

1. Databehandleren bistår, under hensyntagen til behandlingens karakter, så vidt muligt den dataansvarlige ved hjælp af passende tekniske og organisatoriske foranstaltninger med opfyldelse af den dataansvarliges forpligtelse til at besvare anmodninger om udøvelsen af de registreredes rettigheder som fastlagt i databeskyttelsesforordningens kapitel III.

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

   a. oplysningspligten ved indsamling af personoplysninger hos den registrerede
   b. oplysningspligten, hvis personoplysninger ikke er indsamlet hos den registrerede
   c. Indsigtsretten
   d. retten til berigtigelse
   e. retten til sletning (”retten til at blive glemt”)
   f. retten til begrænsning af behandling
   g. underretningspligten i forbindelse med berigtigelse eller sletning af personoplysninger eller begrænsning af behandling
   h. retten til dataportabilitet
   i. retten til indsigelse
   j. retten til ikke at være genstand for en afgørelse, der alene er baseret på automatisk behandling, herunder profilering

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:
   a. den dataansvarliges forpligtelse til uden unødig forsinkelse og om muligt senest 72 timer, efter at denne er blevet bekendt med det, at anmelde brud på persondatasikkerheden til den kompetente tilsynsmyndighed, den for den dataansvarlige kompetente tilsynsmyndighed (lead supervisory authority), medmindre at det er usandsynligt, at bruddet på persondatasikkerheden indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder

   b. den dataansvarliges forpligtelse til uden unødig forsinkelse at underrette den registrerede om brud på persondatasikkerheden, når bruddet sandsynligvis vil medføre en høj risiko for fysiske personers rettigheder og frihedsrettigheder

   c. den dataansvarliges forpligtelse til forud for behandlingen at foretage en analyse af de påtænkte behandlingsaktiviteters konsekvenser for beskyttelse af personoplysninger (en konsekvensanalyse)

d. den dataansvarliges forpligtelse til at høre den kompetente tilsynsmyndighed, den for den dataansvarlige kompetente tilsynsmyndighed (lead supervisory authority), 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.

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

1. Databehandleren underretter uden unødig forsinkelse den dataansvarlige efter at være blevet opmærksom på, at der er sket et brud på persondatasikkerheden.

2. Databehandlerens underretning til den dataansvarlige skal om muligt ske senest 24 timer efter, 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. databeskyttelsesforordningens artikel 33.

3. I overensstemmelse med Bestemmelse 9.2.a 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:

    a. karakteren af bruddet på persondatasikkerheden, herunder, hvis det er muligt, kategorierne og det omtrentlige antal berørte registrerede samt kategorierne og det omtrentlige antal berørte registreringer af personoplysninger

    b. de sandsynlige konsekvenser af bruddet på persondatasikkerheden

    c. 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.

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

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 medlemsstaternes nationale ret foreskriver opbevaring af personoplysningerne.

   Databehandleren forpligter sig til alene at behandle personoplysningerne til de(t) formål, i den periode og under de betingelser, som disse regler foreskriver.

12.Revision, herunder inspektion

1. Databehandleren stiller alle oplysninger, der er nødvendige for at påvise overholdelsen af databeskyttelsesforordningens 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.

2. Procedurerne for den dataansvarliges revisioner, herunder inspektioner, med databehandleren og underdatabehandlere er nærmeret angivet i Bilag C.7. og C.8.

3. Databehandleren er forpligtet til at give tilsynsmyndigheder, som efter gældende lovgivningen 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

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 databeskyttelsesforordningen.

14.Ikrafttræden og ophør

1. Bestemmelserne træder i kraft på datoen for begge parters underskrift heraf.

2. Begge parter kan kræve Bestemmelserne genforhandlet, hvis lovændringer eller uhensigtsmæssigheder i Bestemmelserne giver anledning hertil.

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.

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.

5. Underskrift

   På vegne af den dataansvarlige

   Navn:_____

   Stilling: _____

   Telefonnummer: _____

   E-mail: _____

   Underskrift: _____

   På vegne af databehandleren

   Navn: Tristan White
   Stilling: CEO
   Telefonnummer: +45 26 81 83 48
   E-mail: tw@senbee.com

   Underskrift: 

15.Kontaktpersoner hos den dataansvarlige og databehandleren

Parterne kan kontakte hinanden via nedenstående kontaktpersoner.

Parterne er forpligtet til løbende at orientere hinanden om ændringer vedrørende kontaktpersoner.

Den dataansvarlige

Navn: _____

Stilling: _____

Telefonnummer: _____

E-mail: _____

Databehandleren

Navn: Tristan White
Stilling: CEO
Telefonnummer: +45 26 81 83 48
E-mail: tw@senbee.com

Bilag A - Oplysninger om behandlingen

A.1. Formålet med databehandlerens behandling af personoplysninger på vegne af den dataansvarlige

Databehandleren behandler personoplysninger med henblik på at levere, drifte og vedligeholde Senbee-platformen i henhold til den dataansvarliges instrukser, herunder understøttelse af platformens funktioner, administration, brugerstyring, support, fejlsøgning, sikkerhed samt logning.

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

Behandlingen omfatter registrering, strukturering, lagring, tilpasning, søgning, visning, videregivelse (til autoriserede brugere og eventuelle underdatabehandlere), sammenstilling, begrænsning og sletning af personoplysninger i forbindelse med brug af Senbee-platformen.

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

Navn, e-mailadresse, telefonnummer, organisatorisk tilknytning (virksomhed, afdeling, rolle), bruger-id, adgangs- og aktivitetslogdata (fx login, handlinger i platformen), samt øvrige oplysninger som den dataansvarlige vælger at registrere eller uploade i Senbee-platformen (fx fritekstfelter, noter og vedhæftninger), samt adgangs- og besøgsrelaterede oplysninger i det omfang den dataansvarlige anvender platformens funktioner hertil..

A.4. Behandlingen omfatter følgende kategorier af registrerede

Brugere oprettet af den dataansvarlige i Senbee-platformen, herunder den dataansvarliges medarbejdere, administratorer og øvrige interne brugere, samt eksterne brugere som den dataansvarlige giver adgang, fx lejere, gæster/besøgende, leverandørkontakter og andre samarbejdspartnere.

A.5. Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige kan påbegyndes efter disse Bestemmelsers ikrafttræden. Behandlingen har følgende varighed

Behandlingen pågår i aftaleperioden, dvs. så længe databehandleren leverer tjenester til den dataansvarlige. Ved ophør af tjenesterne ophører behandlingen, og personoplysninger håndteres herefter i overensstemmelse med bestemmelse 11 om sletning og returnering.

Bilag B - Underdatabehandlere

B.1. Godkendte underdatabehandlere

Ved Bestemmelsernes ikrafttræden har den dataansvarlige godkendt brugen af følgende underdatabehandlere:

Navn	Land	Beskrivelse af behandling
Google Workspace	United States	Drift af kontor- og samarbejdsværktøjer (mail, dokumenter mv.) for Senbees interne operationer.
UpCloud	Finland	Hosting/drift som del af Senbees operationer.
SMTP2GO	New Zealand	Afsendelse af e-mail (fx notifikationer).
GatewayAPI	Denmark	Afsendelse af SMS (fx notifikationer).
Economic	Denmark	Økonomisystem til interne operationer.
Slack	United States	Intern kommunikation som del af Senbees operationer.
Pipedrive	United States	CRM til interne operationer.
Featurebase	Estonia	Live chat og feedback-funktionalitet i platformen.

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

C.1. Behandlingens genstand/instruks

Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige sker ved, at databehandleren udfører følgende:

Databehandleren instrueres i at behandle personoplysninger i det omfang det er nødvendigt for at levere, drifte, vedligeholde og supportere Senbee-platformen i overensstemmelse med aftalen, herunder:

- at hoste og lagre data (i cloud eller i den dataansvarliges miljø ved on-prem)
- at gøre data tilgængelige for den dataansvarliges autoriserede brugere via platformens funktioner
- at administrere brugeradgange og roller efter den dataansvarliges instrukser
- at foretage logning, overvågning og fejlsøgning af drifts- og sikkerhedshensyn
- at udføre backup, gendannelse og sletning/returnering ved ophør
- at yde teknisk support og vedligeholdelse, herunder fejlretning og opdateringer

C.2. Behandlingssikkerhed

Sikkerhedsniveauet skal afspejle:

Behandlingen omfatter almindelige personoplysninger vedrørende brugere og kontaktpersoner samt bruger- og aktivitetsdata. Behandlingen kan omfatte oplysninger, som den dataansvarlige selv indtaster eller uploader i platformen. Som udgangspunkt er platformen ikke tiltænkt behandling af særlige kategorier af personoplysninger eller oplysninger om strafbare forhold. Sikkerhedsniveauet fastsættes på baggrund af behandlingens karakter, omfang, sammenhæng og formål samt risici af varierende sandsynlighed og alvor for registreredes rettigheder og frihedsrettigheder, og vurderes som et passende højt sikkerhedsniveau for en professionel B2B SaaS-løsning.

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

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

Krav til pseudonymisering og kryptering
Personoplysninger krypteres under transmission (TLS eller tilsvarende). Personoplysninger krypteres ved lagring i relevante systemer, hvor dette er teknisk muligt og risikobaseret hensigtsmæssigt. Sikkerhedsoplysninger som adgangskoder opbevares som envejshash.

Pseudonymisering anvendes, hvor det er relevant for at reducere risiko ved logning og fejlsøgning.

Vedvarende fortrolighed, integritet, tilgængelighed og robusthed
Adgang til personoplysninger begrænses efter need-to-know og mindst mulige rettigheder, herunder rollebaseret adgangsstyring. Administrative adgange beskyttes med stærk autentifikation. Ændringer i systemer og konfigurationer styres og dokumenteres. Sikkerhedsopdateringer og sårbarheder håndteres efter fastlagte processer. Der gennemføres organisatoriske foranstaltninger, herunder sikkerhedspolitikker, træning og håndtering af leverandører.

Rettidig gendannelse ved fysisk eller teknisk hændelse
Der udføres sikkerhedskopiering og der etableres procedurer for gendannelse af data og systemer. Backup og restore testes regelmæssigt. Ved on-prem leverance fastlægges backup og gendannelsesansvar i aftalegrundlaget, og databehandler yder bistand efter behov.

Regelmæssig afprøvning, vurdering og evaluering
Der gennemføres løbende risikovurderinger og sikkerhedsreview af relevante kontroller. Effektiviteten af tekniske og organisatoriske foranstaltninger vurderes regelmæssigt, herunder via interne kontroller, leverandørvurderinger samt test af backup/restore og relevante sikkerhedsforanstaltninger.

Adgang via internettet
Adgang til platformen sker via sikre forbindelser (HTTPS/TLS). Sessionsstyring og beskyttelse mod uautoriseret adgang implementeres, herunder rate limiting hvor relevant. Den dataansvarlige er ansvarlig for korrekt adgangsstyring af egne brugere.

Beskyttelse under transmission
Data transmitteres krypteret med TLS eller tilsvarende. Integrationskald og API-adgang sikres med passende autentifikationsmekanismer (fx tokens eller nøgler) og begrænses efter behov.

Beskyttelse under opbevaring
Data opbevares i systemer med adgangskontrol, logning og passende beskyttelse mod uautoriseret adgang. Kryptering ved lagring anvendes hvor relevant. Sikkerhedskopier opbevares beskyttet og adgangen begrænses.

Fysisk sikring af lokaliteter
For cloud leverance sker fysisk sikring gennem datacenterleverandørens kontroller. For on-prem leverance er den dataansvarlige ansvarlig for fysisk sikring af den infrastruktur, hvor behandlingen sker, medmindre andet er aftalt.

Hjemme- og fjernarbejdspladser
Databehandlerens personale kan arbejde fjernbaseret under kontrollerede forhold, herunder

krav om skærmlås, opdaterede enheder, kryptering af enheder hvor relevant, sikker netværksadgang og overholdelse af interne politikker for fjernarbejde.

Logging
Der foretages logning af relevante sikkerheds- og driftsmæssige hændelser, herunder autentifikation, administrative handlinger og væsentlige ændringer. Logadgang begrænses, og logs beskyttes mod uautoriseret ændring. Logopbevaring og adgang vurderes risikobaseret.

C.3 Bistand til den dataansvarlige

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:

Databehandleren bistår den dataansvarlige med at opfylde sine forpligtelser efter databeskyttelsesreglerne i det omfang, det vedrører databehandlerens behandling og med hensyn til behandlingens art og de oplysninger, der er tilgængelige for databehandleren. Bistand ydes som udgangspunkt gennem platformens standardfunktionalitet og standarddokumentation. Bistand, der kræver væsentlige ekstra ressourcer, udvikling eller særskilte undersøgelser, kan ydes mod særskilt aftale og vederlag.

Databehandleren gennemfører følgende foranstaltninger for at bistå den dataansvarlige:

- stiller relevant information om behandlingen og sikkerhedsforanstaltninger til rådighed, herunder oplysninger om anvendte underdatabehandlere
- understøtter håndtering af registreredes rettigheder ved at muliggøre søgning, udtræk/eksport, rettelse og sletning i det omfang dette understøttes af platformens funktioner
- bistår ved sikkerhedshændelser ved at underrette og fremsende tilgængelige oplysninger om hændelsen, berørte data og iværksatte afhjælpende foranstaltninger
- bistår ved DPIA og eventuel forudgående høring ved at stille relevante oplysninger til rådighed om behandlingen og de tekniske og organisatoriske foranstaltninger, i det omfang det vedrører databehandlerens leverance

C.4 Opbevaringsperiode/sletterutine

Personoplysninger opbevares i produktionsmiljøet i aftaleperioden og så længe den dataansvarlige har en aktiv konto og anvender tjenesterne. Ved ophør af tjenesten vedrørende behandling af personoplysninger tilbageleverer databehandleren personoplysningerne i et almindeligt anvendt, maskinlæsbart format efter anmodning og sletter herefter personoplysningerne i overensstemmelse med bestemmelse 11.1.

Sikkerhedskopier kan indeholde personoplysninger i en begrænset periode efter sletning/ophør som led i databehandlerens normale backup-rotation i op til 30 dage, hvorefter de slettes eller overskrives. Personoplysninger i sikkerhedskopier gøres ikke aktivt tilgængelige, medmindre det er nødvendigt for gendannelse.

Ved on-prem leverance opbevares og slettes personoplysninger i den dataansvarliges miljø efter den dataansvarliges instrukser og konfiguration, og databehandler yder bistand til eksport og sletning efter behov.

C.5 Lokalitet for behandling

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

Behandling kan finde sted på følgende lokaliteter:

1. Cloud leverance: I databehandlerens hostingmiljø i EU (primært Tyskland) anvendt af databehandleren og/eller underdatabehandlere angivet i bilag B (fx hosting- og driftsleverandør).
2. On-prem leverance: I den dataansvarliges egne lokaliteter og/eller hostingmiljø, som den dataansvarlige stiller til rådighed, hvor databehandlerens adgang kan ske fjernbaseret efter den dataansvarliges instrukser.
3. Support og drift: Hos databehandleren (Senbee A/S) og relevante underdatabehandlere angivet i bilag B, i det omfang det er nødvendigt for support, fejlsøgning, sikkerhed og vedligeholdelse

C.6 Instruks vedrørende overførsel af personoplysninger til tredjelande

Databehandleren må kun overføre personoplysninger til tredjelande eller internationale organisationer i det omfang dette er nødvendigt for leveringen af tjenesterne, og kun når (i) overførslen sker i overensstemmelse med den dataansvarliges dokumenterede instrukser og (ii) et gyldigt overførselsgrundlag efter databeskyttelsesforordningens kapitel V foreligger.

Overførsel kan ske til de tredjelande, hvor databehandlerens underdatabehandlere eller deres behandlingslokationer er etableret, jf. bilag B og databehandlerens til enhver tid opdaterede underdatabehandlerliste.

Overførselsgrundlaget er, afhængigt af den konkrete underdatabehandler og behandlingslokation:

a) Europa-Kommissionens afgørelse om tilstrækkeligt beskyttelsesniveau (GDPR artikel 45), hvor relevant, eller
b) Europa-Kommissionens Standard Contractual Clauses (SCC) (GDPR artikel 46, stk. 2, litra c), suppleret med relevante tekniske og organisatoriske foranstaltninger baseret på en risikovurdering, eller
c) for overførsler til USA: EU-US Data Privacy Framework (GDPR artikel 45), hvor modtageren er certificeret herunder, ellers SCC efter litra b.

Ved on-prem leverance sker der som udgangspunkt ingen tredjelandsoverførsler fra den dataansvarliges miljø, medmindre den dataansvarlige selv konfigurerer eller instruerer integrationer eller underdatabehandlere, der medfører en sådan overførsel.

Hvis den dataansvarlige ikke i disse Bestemmelser eller efterfølgende giver en dokumenteret instruks vedrørende overførsels af personoplysninger til et tredjeland, er databehandleren ikke berettiget til inden for rammerne af disse Bestemmelser at foretage sådanne overførsler.

C.7 Procedurer for den dataansvarliges revisioner, herunder inspektioner, med behandlingen af personoplysninger, som er overladt til databehandleren

Databehandleren skal én gang årligt for egen regning regning indhente en revisionsrapport eller erklæring fra en uafhængig tredjepart vedrørende databehandlerens overholdelse af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse Bestemmelser.

Der er enighed mellem parterne om, at følgende typer af revisionsrapport eller erklæring kan anvendes i overensstemmelse med disse Bestemmelser: ISO 27001-certifikat, ISAE 3000/3402-erklæring, SOC 2 Type II-rapport eller tilsvarende uafhængig tredjeparts revisionsrapport/inspektionsrapport, der dækker relevante tekniske og organisatoriske foranstaltninger.

Revisionsrapporter eller erklæringer fremsendes uden unødig forsinkelse til den dataansvarlige til orientering. Den dataansvarlige kan anfægte rammerne for og/eller metoden i revisionsrapporten eller erklæringen og kan i sådanne tilfælde anmode om en ny revisionsrapport eller inspektionsrapport under andre rammer og/eller under anvendelse af anden metode.

Baseret på resultaterne af revisionsrapporten eller erklæringen, er den dataansvarlige berettiget til at anmode om gennemførelse af yderligere foranstaltninger med henblik på at sikre overholdelsen af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse Bestemmelser.

Den dataansvarlige eller en repræsentant for den dataansvarlige har herudover adgang til at foretage inspektioner, herunder fysiske inspektioner, med lokaliteterne hvorfra databehandleren foretager behandling af personoplysninger, herunder fysiske lokaliteter og systemer, der benyttes til eller i forbindelse med behandlingen. Sådanne inspektioner kan gennemføres, når den dataansvarlige finder det nødvendigt."

Den dataansvarliges eventuelle udgifter i forbindelse med en fysisk inspektion afholdes af den dataansvarlige selv. Databehandleren er dog forpligtet til at afsætte de ressourcer (hovedsageligt den tid), der er nødvendig(e) for, at den dataansvarlige kan gennemføre sin inspektion.

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

Databehandleren indhenter og gennemgår som udgangspunkt underdatabehandlernes uafhængige tredjeparts revisionsrapporter og/eller certificeringer. Relevant dokumentation stilles til rådighed for den dataansvarlige efter anmodning. Fysiske inspektioner hos underdatabehandlere gennemføres alene i det omfang, det er muligt efter underdatabehandlerens vilkår.

Databehandleren skal én gang årligt for underdatabehandlerens regning indhente en revisionsrapport eller erklæring fra en uafhængig tredjepart vedrørende underdatabehandlerens overholdelse af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse Bestemmelser.

Der er enighed mellem parterne om, at følgende typer af revisionsrapporter eller erklæringer kan anvendes i overensstemmelse med disse bestemmelser: SOC 2 Type II, ISAE 3000/3402, ISO 27001-certificering eller tilsvarende uafhængig tredjeparts revisionsrapport/inspektionsrapport.

revisionsrapporten eller erklæringen fremsendes uden unødig forsinkelse til den dataansvarlige til orientering. Den dataansvarlige kan anfægte rammerne for og/eller metoden i revisionsrapporten eller erklæringen og kan i sådanne tilfælde anmode om en ny revisionsrapport eller inspektionsrapport under andre rammer og/eller under anvendelse af anden metode.

Baseret på resultaterne af revisionsrapporten eller erklæring, er den dataansvarlige berettiget til at anmode om gennemførelse af yderligere foranstaltninger med henblik på at sikre overholdelsen af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse Bestemmelser.

Databehandleren eller en repræsentant for databehandleren har herudover adgang til at foretage inspektioner, herunder fysiske inspektioner, med lokaliteterne hvorfra underdatabehandleren foretager behandling af personoplysninger, herunder fysiske lokaliteter og systemer, der benyttes til eller i forbindelse med behandlingen. Sådanne inspektioner kan gennemføres, når databehandleren (eller den dataansvarlige) finder det nødvendigt.

Dokumentation for sådanne inspektioner fremsendes uden unødig forsinkelse til den dataansvarlige til orientering. Den dataansvarlige kan anfægte rammerne for og/eller metoden af inspektionen og kan i sådanne tilfælde anmode om gennemførelsen af en ny inspektion under andre rammer og/eller under anvendelse af anden metode.