Standardkontraktsbestemmelser

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

mellem den juridiske enhed, som opretter en konto på Penpally-platformen
herefter "den dataansvarlige"

og

Penpally (Gustav Søgård Holding ApS)
CVR 44071657
Tyrolsgade 19, 4th,
2300 København S,
Danmark

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 Penpally SaaS-løsningen 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 tre 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[1] 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.

1 Henvisninger til "medlemsstat" i disse bestemmelse skal forstås som en henvisning til "EØS medlemsstater".

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.

   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. Dog kan et kortere varsel anvendes, såfremt en udskiftning af en underdatabehandler er påkrævet af presserende og uforudsete sikkerhedsmæssige eller driftskritiske årsager. I sådanne tilfælde vil underretning ske hurtigst muligt. 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. Databehandleren skal i sin aftale med underdatabehandleren indføje den dataansvarlige som begunstiget tredjemand, således at den dataansvarlige i tilfælde af at databehandleren faktisk eller retligt set er ophørt med at eksistere eller i tilfælde af databehandlerens konkurs, har ret til at opsige underdatabehandleraftalen og instruere underdatabehandleren i at slette eller tilbagelevere personoplysningerne.

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 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, Datatilsynet, 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, Datatilsynet, 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 48 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. Denne Databehandleraftale træder i kraft og anses for juridisk bindende for begge parter, når Kunden accepterer Penpal's Servicevilkår ved oprettelse af en konto. Den dato, hvor Kunden opretter sin konto, udgør aftalens ikrafttrædelsesdato.

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.

15. Kontaktpersoner hos databehandleren

Navn	Gustav Søgård
Stilling	Stifter
Telefonnummer	+45 28 66 22 46
E-mail	info@penpally.dk

Bilag A Oplysninger om behandlingen

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

Formålet med databehandlerens behandling af personoplysninger er at muliggøre Leverandørens (Penpally) levering af en AI-drevet e-mail-assistenttjeneste til Kunden, som genererer personaliserede e-mailudkast til gæstekommunikation. Dette inkluderer at modtage gæsteoplysninger fra Kundens Property Management System (PMS) og e-mailklienter med det formål at udarbejde, præsentere og opdatere e-mailudkast til Kundens godkendelse og afsendelse til gæsterne.

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

Behandlingen består primært af:

- Indsamling/modtagelse af personoplysninger fra Kundens PMS og e-mailklienter (via integration).
- Opbevaring af disse personoplysninger på sikrede servere.
- Analyse og behandling af personoplysninger ved brug af AI-modeller til generering af e-mailudkast.
- Visning og opdatering af e-mailudkast i Løsningens brugerflade.
- Sletning eller returnering af personoplysninger ved aftalens ophør.

Behandlingen er automatiseret med begrænset manuel indblanding, primært ved opsætning og support.

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

Behandlingen omfatter primært almindelige personoplysninger om Kundens gæster. Dette kan omfatte, men er ikke begrænset til:

- Navn (for- og efternavn)
- Kontaktoplysninger (e-mailadresse, telefonnummer)
- Reservationsoplysninger (f.eks. bookingnummer, ankomst-/afrejsedato, værelsesnummer)
- Præferencer eller specifikke anmodninger relateret til opholdet, som Kunden måtte registrere og videresende via PMS eller e-mailkommunikation.
- Indhold af tidligere e-mailkorrespondance mellem Kunde og gæst.

A.4. Behandlingen omfatter følgende kategorier af registrerede

Behandlingen omfatter primært personoplysninger om Kundens henvendelser og potentielt personer, der kommunikerer med Kunden via e-mail, og hvis e-mailindhold sendes til behandling af Penpally.

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

Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige påbegyndes ved ikrafttrædelsen af disse Bestemmelser og fortsætter, så længe hovedaftalen om levering af Penpally SaaS-løsningen er gældende mellem Parterne.

Bilag B Underdatabehandlere

B.1. Godkendte underdatabehandlere

Ved Bestemmelsernes ikrafttræden har den dataansvarlige godkendt brugen af følgende underdatabehandlere

NAVN	CVR	ADRESSE	BESKRIVELSE AF BEHANDLING
Supabase	N/A	San Francisco, CA 94101, USA (Hovedsæde)	Datalagring og databasefunktionalitet via datacenter i EU (Frankfurt).
OpenAI	N/A	3180 18th Street, San Francisco, CA 94110, USA	Behandling af data via API-kald til generering af AI-email-udkast.
Vercel, Inc.	N/A	440 N Barranca Avenue #4133, Covina, CA 91723, USA	Hosting af webapplikation og håndtering af weblogs for Løsningen.
Intercom, Inc.	N/A	55 2nd Street, 4th Floor, San Francisco, CA 94105, USA	Platform for kundekommunikation og support, herunder chat og e-mail.
Amplitude, Inc.	N/A	201 Third Street, Suite 200, San Francisco, CA 94103, USA	Brugeradfærd- og produktanalyse.
Stripe, Inc.	N/A	354 Oyster Point Blvd, South San Francisco, CA 94080, USA	Betalingsbehandling og abonnementsstyring.
Resend	N/A	548 Market St, PMB 95233, San Francisco, CA 94104, USA	Afsendelse af system-e-mails (transactional emails).

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.

B.2. Varsel for godkendelse af underdatabehandlere

Databehandleren skal skriftligt underrette den dataansvarlige om eventuelle planlagte ændringer vedrørende tilføjelse eller udskiftning af underdatabehandlere med mindst

30 dages varsel i overensstemmelse med Bestemmelse 7.2.

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:

- **Modtagelse og indsamling:** Modtagelse af gæsteoplysninger fra den dataansvarliges Property Management System (PMS) (f.eks. BookVisit, hBook, Mews) og/eller e-mailklienter (f.eks. Gmail, Outlook) med henblik på at facilitere personaliseret e-mailkommunikation.
- **Opbevaring:** Sikker opbevaring af de modtagne personoplysninger på databehandlerens cloud-baserede infrastruktur.
- **Analyse og generering:** Anvendelse af AI-modeller til analyse af gæsteoplysninger og generering af udkast til e-mailkommunikation, herunder f.eks. bekræftelser, velkomst-e-mails, tilbud og service-e-mails.
- **Præsentation og opdatering:** Tilgængeliggørelse af genererede e-mailudkast i Løsningens brugerflade for den dataansvarliges gennemgang og bedømmelse.
- **Sletning og returnering:** Sletning af personoplysninger ved afslutning af databehandlerforholdet, eller efter instruks fra den dataansvarlige, samt bistand til dataeksport.

C.2. Behandlingssikkerhed

Sikkerhedsniveauet skal afspejle:

Behandlingen omfatter almindelige personoplysninger om gæster og kommunikationsdata. Risikoen for de registreredes rettigheder og frihedsrettigheder vurderes at være **moderat til høj**, da brud på persondatasikkerheden kan medføre identitetstyveri, tab af kontrol over egne data, økonomisk tab, skade på omdømme, eller andre betydelige ulemper for de registrerede. Det er afgørende at sikre fortrolighed, integritet og tilgængelighed af personoplysningerne. Der er ingen indikation af behandling af særlige kategorier af personoplysninger (følsomme data) i henhold til GDPR artikel 9.

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:

- **Pseudonymisering og kryptering af personoplysninger:**
    - Personoplysninger skal, hvor det er teknisk muligt og hensigtsmæssigt, pseudonymiseres.
    - Alle personoplysninger skal krypteres under transmission (in transit) ved brug af anerkendte krypteringsprotokoller (f.eks. TLS 1.2+).

  - Alle personoplysninger skal krypteres under opbevaring (at rest) i databaser og fillagringssystemer ved brug af industristandard krypteringsalgoritmer.
- **Evnen til at sikre vedvarende fortrolighed, integritet, tilgængelighed og robusthed af behandlingssystemer og -tjenester:**
  - Adgang til systemer, der behandler personoplysninger, skal være baseret på "least privilege"-princippet (mindst mulig adgang) og "need-to-know"-princippet.
  - Adgangskontrolsystemer med stærke adgangskoder og to-faktor-autentificering (2FA) skal anvendes for al administrativ adgang.
  - Der skal implementeres firewalls, indbrudsdetekteringssystemer (IDS) og indbrudsforebyggelsessystemer (IPS) for at beskytte netværksgrænseflader.
  - Sårbarhedsscanninger og penetrationstests skal udføres regelmæssigt.
- **Evnen til rettidigt at genoprette tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse:**
  - Der skal etableres et fuldt dækkende backup-system med regelmæssig backup af alle personoplysninger.
  - Backup skal opbevares sikkert, geografisk adskilt og krypteret.
- **Procedurer for regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske foranstaltninger til sikring af behandlingssikkerheden:**
  - Regelmæssige interne og/eller eksterne sikkerhedsrevisioner skal udføres for at vurdere overholdelse af sikkerhedspolitikker og -standarder.
  - Leverandøren skal have en proces for løbende at overvåge og vurdere trusselsbilledet samt opdatere sikkerhedsforanstaltninger derefter.
  - Medarbejdere, der behandler personoplysninger, skal modtage regelmæssig træning i informationssikkerhed og databeskyttelse.
- **Adgang til oplysningerne via internettet:**
  - Adgang til Løsningen og underliggende systemer via internettet skal sikres med krypterede forbindelser (HTTPS/TLS) og stærke autentificeringsmekanismer.
  - Der skal anvendes sikre API-adgangspunkter og -nøgler til integration med kundens PMS og e-mailklienter.
- **Beskyttelse af oplysninger under transmission:**
  - Alle dataoverførsler mellem kundens systemer og Penpally, samt mellem Penpally og dens underdatabehandlere, skal ske via krypterede kanaler (f.eks. TLS/SSL).
- **Beskyttelse af oplysninger under opbevaring:**
  - Data skal opbevares i sikrede datacentre, der overholder anerkendte sikkerhedsstandarder (f.eks. ISO 27001).
  - Adgang til opbevarede data skal begrænses til autoriseret personale med et klart defineret behov.
- **Anvendelse af hjemme-/fjernarbejdspladser:**
  - Medarbejdere, der arbejder eksternt, skal anvende sikre VPN-forbindelser for at få adgang til virksomhedens netværk og systemer.
  - Der skal være klare politikker for brug af egne enheder (BYOD) og for sikkerhed af hjemmearbejdspladser, herunder beskyttelse mod uautoriseret adgang til enheder med adgang til personoplysninger.
- **Logning:**
  - Alle relevante adgange, ændringer og behandlingsaktiviteter i systemerne, der omfatter personoplysninger, skal logges.
  - Logfiler skal sikres mod manipulation, opbevares i en passende periode og gennemgås regelmæssigt for at opdage uregelmæssigheder.

C.3 Bistand til den dataansvarlige

Databehandleren skal så vidt muligt bistå den dataansvarlige i overensstemmelse med Bestemmelse 9.1 og 9.2.

Omfang, udstrækning og omkostninger for bistanden: Databehandlerens bistand ydes for at understøtte den dataansvarliges opfyldelse af sine forpligtelser i henhold til databeskyttelsesforordningen.

Bistand, der kan ydes via Løsningens standardfunktionalitet (f.eks. til eksport og sletning af data), er inkluderet i aftalen. Anmodninger fra den dataansvarlige, der kræver betydelig manuel sagsbehandling eller teknisk udvikling fra databehandlerens side (estimeret til mere end 2 timer pr. sag), vil blive anset som en særskilt ydelse. En sådan ydelse vil blive faktureret efter den dataansvarliges forudgående skriftlige godkendelse baseret på databehandlerens gældende timepris på 400 DKK. Dette gælder ikke, hvis bistanden skyldes databehandlerens misligholdelse af aftalen.

Specifikke tekniske og organisatoriske foranstaltninger:

1. **Bistand ved udøvelse af registreredes rettigheder (jf. Bestemmelse 9.1):**
    - *Teknisk bistand:* Tilbyde funktioner i Løsningen, der understøtter den dataansvarlige i at finde, eksportere eller slette data om specifikke registrerede.
    - *Organisatorisk bistand:* Give vejledning og support, der hjælper den dataansvarlige med at navigere i Løsningen for at imødekomme anmodninger.
    - *Videresendelse af anmodninger:* Videresende enhver anmodning fra registrerede, som databehandleren modtager direkte, til den dataansvarlige uden unødig forsinkelse.
2. **Bistand ved brud på persondatasikkerheden (jf. Bestemmelse 9.2.a og 10):**
    - *Underretning:* Underrette den dataansvarlige i henhold til de aftalte tidsfrister.
    - *Information til anmeldelse:* Tilvejebringe relevant og tilgængelig information om bruddet, herunder, hvis muligt, bruddets art, antal berørte, sandsynlige konsekvenser og trufne foranstaltninger.
    - *Dokumentation:* Føre en intern fortegnelse over alle brud på persondatasikkerheden.
3. **Bistand ved konsekvensanalyser (DPIA) og forudgående høringer (jf. Bestemmelse 9.2.c og 9.2.d):**
    - *Tilgængelighed af information:* Stille relevant information om Løsningens funktioner, sikkerhedsforanstaltninger og databehandlingsprocesser til rådighed, som er nødvendig for den dataansvarliges udførelse af en DPIA.

C.4 Opbevaringsperiode/sletterutine

Personoplysninger behandlet af databehandleren på vegne af den dataansvarlige opbevares, så længe hovedaftalen om levering af Penpally SaaS-løsningen er gældende mellem Parterne.

Ved ophør af tjenesten vedrørende behandling af personoplysninger, skal databehandleren **tilbagelevere alle personoplysningerne til den dataansvarlige og slette eksisterende kopier**, i overensstemmelse med Bestemmelse 11.1. Databehandleren skal bekræfte over for den dataansvarlige, at alle relevante personoplysninger er slettet.

Sletning af data vil ske **senest 30 dage** efter fuldført tilbagelevering af data til den dataansvarlige, medmindre længere opbevaring er påkrævet i henhold til EU-ret eller medlemsstaternes nationale ret.

Databehandleren opretholder interne procedurer, der sikrer, at personoplysninger slettes eller anonymiseres, når de ikke længere er nødvendige for formålet med behandlingen eller for at overholde lovmæssige krav.

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:

- **Primære lokaliteter (Databehandlerens egne faciliteter/kontor):**
  - **Adresse:** Tyrolsgade 19, 4th, 2300 København S, Danmark
  - **Anvendes af:** Penpally (Gustav Søgård Holding ApS)
- **Underdatabehandleres lokaliteter:**
  - **Datacenterlokaliteter for Supabase:**
    - **Lokation:** EU (Frankfurt, Tyskland - eu-central-1)
    - **Anvendes af:** Supabase (som underdatabehandler for datalagring og databasefunktionalitet)
  - **Datacenterlokaliteter for OpenAI:**
    - **Lokation:** USA (San Francisco, CA)
    - **Anvendes af:** OpenAI (som underdatabehandler for AI-behandling og generering af e-mailudkast)
  - **Datacenterlokaliteter for Vercel Inc.:**
    - **Lokation:** USA (San Francisco, CA)
    - **Anvendes af:** Vercel Inc. (som underdatabehandler for hosting af webapplikation og håndtering af weblogs for Løsningen)
  - **Datacenterlokaliteter for Intercom, Inc.:**
    - **Lokation:** USA (San Francisco, CA)
    - **Anvendes af:** Intercom, Inc. (som underdatabehandler for platform for kundekommunikation og support, herunder chat og e-mail)
  - **Datacenterlokaliteter for Amplitude, Inc.:**
    - **Lokation:** USA (San Francisco, CA)
    - **Anvendes af:** Amplitude, Inc. (som underdatabehandler for brugeradfærd- og produktanalyse)

C.6 Instruks vedrørende overførsel af personoplysninger til tredjelande

Databehandleren er instrueret i at overføre personoplysninger til USA i det omfang, det er nødvendigt for levering af Penpally SaaS-løsningen, og under forudsætning af at et gyldigt overførselsgrundlag i henhold til GDPR kapitel V er sikret for hver overførsel.

Specifik instruks og grundlag for overførsel:

1. Overførsler baseret på EU-Kommissionens tilstrækkelighedsafgørelse (GDPR art. 45)

Overførsel af personoplysninger til følgende modtagere i USA sker på baggrund af EU-Kommissionens tilstrækkelighedsafgørelse for EU-U.S. Data Privacy Framework (DPF):

- **Modtagere:**
  - **Vercel Inc.:** For hosting af webapplikation og håndtering af weblogs for Løsningen.
  - **Intercom, Inc.:** For platform for kundekommunikation og support, herunder chat og e-mail.
  - **Amplitude, Inc.:** For brugeradfærd- og produktanalyse.
  - **Stripe, Inc.:** For betalingsbehandling og abonnementsstyring.
  - **Resend:** For afsendelse af system-e-mails (transactional emails).
- **Databehandlerens forpligtelse:** Databehandleren forpligter sig til at sikre, at disse underdatabehandlere opretholder deres aktive certificering under DPF-ordningen i hele aftalens løbetid. Databehandleren skal på anmodning fra den dataansvarlige kunne dokumentere underdatabehandlerens aktive certificering.

2. Overførsler baseret på Standardkontraktbestemmelser (GDPR art. 46)

Overførsel af personoplysninger til følgende modtager i USA sker på baggrund af EU-Kommissionens standardkontraktbestemmelser (Standard Contractual Clauses - SCCs):

- **Modtager:**
  - **OpenAI:** For AI-behandling og generering af e-mailudkast som en del af Penpally SaaS-løsningen.
- **Databehandlerens forpligtelse:** Databehandleren garanterer at have indgået gyldige SCCs med OpenAI. Databehandleren skal, på anmodning fra den dataansvarlige, stille en kopi af de indgåede SCCs til rådighed for den dataansvarlige som dokumentation for, at det fornødne overførselsgrundlag er etableret.

Generelt

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.

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

Databehandleren anerkender den dataansvarliges ret til revision for at påvise overholdelse af databeskyttelsesforordningen og denne aftale.

Databehandleren har som mål at opnå en anerkendt, uafhængig tredjepartsrevisionserklæring (f.eks. ISAE 3000) for at dokumentere sit sikkerhedsniveau.

Indtil en sådan ekstern erklæring foreligger, giver databehandleren på anmodning den dataansvarlige indsigt i sin interne dokumentation for overholdelse af sikkerhedsforanstaltningerne beskrevet i Bilag C.2.

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

Databehandleren er ansvarlig for at sikre, at underdatabehandlere, der anvendes i forbindelse med levering af Ydelserne, overholder de samme databeskyttelsesforpligtelser som dem, der fremgår af denne Databehandleraftale, jf. Bestemmelse 7.3.

For at påvise overholdelsen af underdatabehandleres forpligtelser gælder følgende:

1. **Revisionserklæringer fra tredjepart:** Databehandleren forpligter sig til at indhente og opbevare relevant dokumentation (f.eks. ISAE 3000 Type 2, ISAE 3402 Type 2 erklæringer, ISO 27001-certificeringer eller lignende tredjepartsrevisionsrapporter) fra sine underdatabehandlere. Denne dokumentation bekræfter underdatabehandlerens overholdelse af gældende databeskyttelseslovgivning og de aftalte sikkerhedsstandarder.
2. **Tilgængelighed for den dataansvarlige:** Databehandleren vil på skriftlig anmodning fra den dataansvarlige stille relevant dokumentation om underdatabehandleres compliance til rådighed for den dataansvarlige til gennemgang. Dette omfatter dog ikke kommercielt fortrolige oplysninger i underdatabehandleres aftaler.
3. **Databehandlerens ansvar for tilsyn:** Databehandleren har det primære ansvar for at føre tilsyn med sine underdatabehandlere. Den dataansvarliges eventuelle ønske om direkte inspektion hos en underdatabehandler skal koordineres via databehandleren og kan kun ske med databehandlerens forudgående skriftlige godkendelse og på vilkår, der sikrer fortrolighed og den underdatabehandlerens drift. Eventuelle omkostninger forbundet med en sådan direkte inspektion afholdes af den dataansvarlige.