Databehandleravtale

Mal (uten kunde)

Den danske utgaven er den juridisk gjeldende; denne oversettelsen er kun til orientering.

Standardkontraktsbestemmelser i henhold til artikkel 28 nr. 3 i forordning (EU) 2016/679 (personvernforordningen) for databehandlerens behandling av personopplysninger

Standardavtale fra Datatilsynet, den danske personvernmyndigheten (januar 2020), med Svarflows vedlegg A–D · Versjon 2026-11 · Gjelder fra 19. november 2026

mellom

Den behandlingsansvarlige

[Den behandlingsansvarliges juridiske navn]

CVR [CVR-nummer]

[Adresse]

[Postnummer og sted]

[Land]

heretter «den behandlingsansvarlige»

Databehandleren

Svarflow ApS

CVR 46871421

Danmark

heretter «databehandleren»

som hver for seg er en «part» og sammen utgjør «partene»

HAR AVTALT følgende standardkontraktsbestemmelser (Bestemmelsene) for å overholde personvernforordningen og sikre vern av privatlivets fred og fysiske personers grunnleggende rettigheter og friheter.

1. Innhold

2. Innledning

3. Den behandlingsansvarliges rettigheter og plikter

4. Databehandleren handler etter instruks

5. Konfidensialitet

6. Behandlingssikkerhet

7. Bruk av underdatabehandlere

8. Overføring til tredjeland eller internasjonale organisasjoner

9. Bistand til den behandlingsansvarlige

10. Varsling om brudd på personopplysningssikkerheten

11. Sletting og tilbakelevering av opplysninger

12. Revisjon, herunder inspeksjon
13. Partenes avtale om andre forhold
14. Ikrafttredelse og opphør
15. Kontaktpersoner hos den behandlingsansvarlige og databehandleren
Vedlegg A — Opplysninger om behandlingen
Vedlegg B — Underdatabehandlere
Vedlegg C — Instruks om behandling av personopplysninger
Vedlegg D — Partenes regulering av andre forhold

2. Innledning

2.1 Disse Bestemmelsene fastsetter databehandlerens rettigheter og plikter når denne behandler personopplysninger på vegne av den behandlingsansvarlige.

2.2 Disse Bestemmelsene er utformet med sikte på at partene skal overholde artikkel 28 nr. 3 i europaparlaments- og rådsforordning (EU) 2016/679 av 27. april 2016 om vern av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger samt om oppheving av direktiv 95/46/EF (personvernforordningen).

2.3 I forbindelse med leveringen av AI-telefonresepsjonisten Nora med tilhørende booking, beskjeder og SMS-bekreftelser (heretter «Tjenesten») behandler databehandleren personopplysninger på vegne av den behandlingsansvarlige i samsvar med disse Bestemmelsene.

2.4 Bestemmelsene har forrang foran eventuelle tilsvarende bestemmelser i andre avtaler mellom partene.

2.5 Disse Bestemmelsene har fire vedlegg, og vedleggene utgjør en integrert del av Bestemmelsene.

2.6 Vedlegg A inneholder nærmere opplysninger om behandlingen av personopplysninger, herunder om behandlingens formål og art, typen personopplysninger, kategoriene av registrerte og behandlingens varighet.

2.7 Vedlegg B inneholder den behandlingsansvarliges vilkår for databehandlerens bruk av underdatabehandlere og en liste over underdatabehandlere som den behandlingsansvarlige har godkjent bruken av.

2.8 Vedlegg C inneholder den behandlingsansvarliges instruks når det gjelder databehandlerens behandling av personopplysninger, en beskrivelse av de sikkerhetstiltakene som databehandleren som et minimum skal gjennomføre, og hvordan det føres tilsyn med databehandleren og eventuelle underdatabehandlere.

2.9 Vedlegg D inneholder bestemmelser om andre aktiviteter som ikke omfattes av Bestemmelsene.

2.10 Bestemmelsene med tilhørende vedlegg skal oppbevares skriftlig, herunder elektronisk, av begge parter.

2.11 Disse Bestemmelsene fritar ikke databehandleren fra plikter som databehandleren er pålagt etter personvernforordningen eller annen lovgivning.

3. Den behandlingsansvarliges rettigheter og plikter

3.1 Den behandlingsansvarlige er ansvarlig for å sikre at behandlingen av personopplysninger skjer i samsvar med personvernforordningen (se forordningens artikkel 24),

personvernbestemmelser i annen EU-rett eller medlemsstatenes nasjonale rett og disse Bestemmelsene. Henvisninger til «medlemsstat» i disse Bestemmelsene skal forstås som en henvisning til EØS-stater.

3.2 Den behandlingsansvarlige har rett og plikt til å treffe beslutninger om til hvilke(t) formål og med hvilke midler personopplysninger kan behandles.

3.3 Den behandlingsansvarlige er blant annet ansvarlig for å sikre at det foreligger et behandlingsgrunnlag for den behandlingen av personopplysninger som databehandleren instrueres om å foreta.

4. Databehandleren handler etter instruks

4.1 Databehandleren kan bare behandle personopplysninger etter dokumentert instruks fra den behandlingsansvarlige, med mindre det kreves i henhold til EU-retten eller medlemsstatenes nasjonale rett som databehandleren er underlagt. Denne instruksen skal være spesifisert i vedlegg A og C. Etterfølgende instruks kan også gis av den behandlingsansvarlige mens personopplysninger behandles, men instruksen skal alltid være dokumentert og oppbevares skriftlig, herunder elektronisk, sammen med disse Bestemmelsene.

4.2 Databehandleren underretter umiddelbart den behandlingsansvarlige dersom en instruks etter databehandlerens oppfatning er i strid med personvernforordningen eller personvernbestemmelser i annen EU-rett eller medlemsstatenes nasjonale rett.

5. Konfidensialitet

5.1 Databehandleren kan bare gi tilgang til personopplysninger som behandles på vegne av den behandlingsansvarlige, til personer som er underlagt databehandlerens instruksjonsmyndighet, som har forpliktet seg til konfidensialitet eller er underlagt en egnet lovbestemt taushetsplikt, og bare i nødvendig omfang. Listen over personer som har fått tilgang, skal gjennomgås løpende. På bakgrunn av denne gjennomgangen kan tilgangen til personopplysninger stenges dersom tilgangen ikke lenger er nødvendig, og personopplysningene skal deretter ikke lenger være tilgjengelige for disse personene.

5.2 Databehandleren skal etter anmodning fra den behandlingsansvarlige kunne påvise at de aktuelle personene som er underlagt databehandlerens instruksjonsmyndighet, er underlagt ovennevnte taushetsplikt.

6. Behandlingssikkerhet

6.1 Personvernforordningens artikkel 32 fastslår at den behandlingsansvarlige og databehandleren, idet det tas hensyn til den tekniske utviklingen, gjennomføringskostnadene og den aktuelle behandlingens art, omfang, formål og sammenhengen den utføres i, samt risikoene av varierende sannsynlighet og alvorlighetsgrad for fysiske personers rettigheter og friheter, gjennomfører egnede tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som er egnet med hensyn til disse risikoene.

6.2 Den behandlingsansvarlige skal vurdere risikoene for fysiske personers rettigheter og friheter som behandlingen utgjør, og gjennomføre tiltak for å møte disse risikoene. Avhengig av hva som er relevant, kan dette omfatte:

a) pseudonymisering og kryptering av personopplysninger

b) evne til å sikre vedvarende konfidensialitet, integritet, tilgjengelighet og robusthet i behandlingssystemene og -tjenestene

c) evne til å gjenopprette tilgjengeligheten og tilgangen til personopplysninger i rett tid dersom

det oppstår en fysisk eller teknisk hendelse

d) en prosess for regelmessig testing, analysering og vurdering av hvor effektive de tekniske og organisatoriske tiltakene for å sikre behandlingens sikkerhet er.

Etter forordningens artikkel 32 skal databehandleren – uavhengig av den behandlingsansvarlige – også vurdere risikoene for fysiske personers rettigheter som behandlingen utgjør, og gjennomføre tiltak for å møte disse risikoene. For denne vurderingen skal den behandlingsansvarlige stille den nødvendige informasjonen til rådighet for databehandleren, slik at databehandleren kan identifisere og vurdere slike risikoer.

6.3 I tillegg skal databehandleren bistå den behandlingsansvarlige med å overholde den behandlingsansvarliges plikt etter forordningens artikkel 32, blant annet ved å stille den nødvendige informasjonen til rådighet for den behandlingsansvarlige om de tekniske og organisatoriske sikkerhetstiltakene som databehandleren allerede har gjennomført i henhold til forordningens artikkel 32, og all annen informasjon som er nødvendig for at den behandlingsansvarlige skal kunne overholde sin plikt etter forordningens artikkel 32.

6.4 Dersom håndteringen av de identifiserte risikoene – etter den behandlingsansvarliges vurdering – krever gjennomføring av flere tiltak enn de tiltakene som databehandleren allerede har gjennomført, skal den behandlingsansvarlige angi de ytterligere tiltakene som skal gjennomføres, i vedlegg C.

7. Bruk av underdatabehandlere

7.1 Databehandleren skal oppfylle vilkårene nevnt i personvernforordningens artikkel 28 nr. 2 og nr. 4 for å benytte en annen databehandler (en underdatabehandler).

7.2 Databehandleren kan dermed ikke benytte en underdatabehandler for å oppfylle disse Bestemmelsene uten forutgående generell skriftlig godkjenning fra den behandlingsansvarlige.

7.3 Databehandleren har den behandlingsansvarliges generelle godkjenning til bruk av underdatabehandlere. Databehandleren skal skriftlig underrette den behandlingsansvarlige om eventuelle planlagte endringer som gjelder tilføyelse eller utskifting av underdatabehandlere, med minst 30 dagers varsel, og dermed gi den behandlingsansvarlige mulighet til å protestere mot slike endringer før de(n) aktuelle underdatabehandleren(e) tas i bruk. Lengre varsel for underretning i forbindelse med spesifikke behandlingsaktiviteter kan angis i vedlegg B. Listen over underdatabehandlere som den behandlingsansvarlige allerede har godkjent, fremgår av vedlegg B.

7.4 Når databehandleren benytter en underdatabehandler for å utføre spesifikke behandlingsaktiviteter på vegne av den behandlingsansvarlige, skal databehandleren, gjennom en kontrakt eller et annet rettslig dokument i henhold til EU-retten eller medlemsstatenes nasjonale rett, pålegge underdatabehandleren de samme personvernforpliktelsene som dem som fremgår av disse Bestemmelsene, der det særlig gis tilstrekkelige garantier for at underdatabehandleren vil gjennomføre de tekniske og organisatoriske tiltakene på en slik måte at behandlingen oppfyller kravene i disse Bestemmelsene og personvernforordningen.

Databehandleren er derfor ansvarlig for å kreve at underdatabehandleren som et minimum overholder databehandlerens plikter etter disse Bestemmelsene og personvernforordningen.

7.5 Underdatabehandleravtale(r) og eventuelle senere endringer i disse sendes – etter anmodning fra den behandlingsansvarlige – i kopi til den behandlingsansvarlige, som dermed har mulighet til å forsikre seg om at tilsvarende personvernforpliktelser som følger av disse Bestemmelsene, er pålagt underdatabehandleren. Bestemmelser om kommersielle vilkår som ikke påvirker det

personvernrettslige innholdet i underdatabehandleravtalen, skal ikke sendes til den behandlingsansvarlige.

7.6 Dersom underdatabehandleren ikke oppfyller sine personvernforpliktelser, forblir databehandleren fullt ansvarlig overfor den behandlingsansvarlige for oppfyllelsen av underdatabehandlerens plikter. Dette påvirker ikke de registrertes rettigheter som følger av personvernforordningen, herunder særlig forordningens artikkel 79 og 82, overfor den behandlingsansvarlige og databehandleren, herunder underdatabehandleren.

8. Overføring til tredjeland eller internasjonale organisasjoner

8.1 Enhver overføring av personopplysninger til tredjeland eller internasjonale organisasjoner kan bare foretas av databehandleren på bakgrunn av dokumentert instruks om dette fra den behandlingsansvarlige og skal alltid skje i samsvar med personvernforordningens kapittel V.

8.2 Dersom overføring av personopplysninger til tredjeland eller internasjonale organisasjoner som databehandleren ikke er blitt instruert om å foreta av den behandlingsansvarlige, kreves i henhold til EU-retten eller medlemsstatenes nasjonale rett som databehandleren er underlagt, skal databehandleren underrette den behandlingsansvarlige om dette rettslige kravet før behandlingen, med mindre den aktuelle retten forbyr slik underretning av hensyn til viktige allmenne interesser.

8.3 Uten dokumentert instruks fra den behandlingsansvarlige kan databehandleren dermed ikke innenfor rammene av disse Bestemmelsene:

a) overføre personopplysninger til en behandlingsansvarlig eller databehandler i et tredjeland eller en internasjonal organisasjon

b) overlate behandling av personopplysninger til en underdatabehandler i et tredjeland

c) behandle personopplysningene i et tredjeland.

8.4 Den behandlingsansvarliges instruks om overføring av personopplysninger til et tredjeland, herunder det eventuelle overføringsgrunnlaget i personvernforordningens kapittel V som overføringen er basert på, skal angis i vedlegg C.6.

8.5 Disse Bestemmelsene skal ikke forveksles med standardpersonvernbestemmelser som nevnt i personvernforordningens artikkel 46 nr. 2 bokstav c og d, og disse Bestemmelsene kan ikke utgjøre et grunnlag for overføring av personopplysninger som nevnt i personvernforordningens kapittel V.

9. Bistand til den behandlingsansvarlige

9.1 Databehandleren bistår, idet det tas hensyn til behandlingens art, så langt det er mulig den behandlingsansvarlige ved hjelp av egnede tekniske og organisatoriske tiltak med å oppfylle den behandlingsansvarliges plikt til å besvare anmodninger om utøvelse av de registrertes rettigheter som fastsatt i personvernforordningens kapittel III.

Dette innebærer at databehandleren så langt det er mulig skal bistå den behandlingsansvarlige i forbindelse med at den behandlingsansvarlige skal sikre overholdelse av:

a) informasjonsplikten ved innsamling av personopplysninger fra den registrerte

b) informasjonsplikten når personopplysninger ikke er samlet inn fra den registrerte

c) retten til innsyn

d) retten til retting

e) retten til sletting («retten til å bli glemt»)

f) retten til begrensning av behandling

g) underretningsplikten i forbindelse med retting eller sletting av personopplysninger eller begrensning av behandling

h) retten til dataportabilitet

i) retten til å protestere

j) retten til ikke å være gjenstand for en avgjørelse som utelukkende er basert på automatisert behandling, herunder profilering.

9.2 I tillegg til databehandlerens plikt til å bistå den behandlingsansvarlige i henhold til bestemmelse 6.3 bistår databehandleren videre, idet det tas hensyn til behandlingens art og de opplysningene som er tilgjengelige for databehandleren, den behandlingsansvarlige med:

a) den behandlingsansvarliges plikt til uten ugrunnet opphold og om mulig senest 72 timer etter å ha fått kjennskap til det å melde brudd på personopplysningssikkerheten til den kompetente tilsynsmyndigheten – for en behandlingsansvarlig i Danmark: Datatilsynet – med mindre det er lite sannsynlig at bruddet på personopplysningssikkerheten vil medføre en risiko for fysiske personers rettigheter eller friheter

b) den behandlingsansvarliges plikt til uten ugrunnet opphold å underrette den registrerte om brudd på personopplysningssikkerheten når bruddet sannsynligvis vil medføre en høy risiko for fysiske personers rettigheter og friheter

c) den behandlingsansvarliges plikt til før behandlingen å foreta en vurdering av hvilke konsekvenser de planlagte behandlingsaktivitetene vil ha for vernet av personopplysninger (en vurdering av personvernkonsekvenser)

d) den behandlingsansvarliges plikt til å rådføre seg med den kompetente tilsynsmyndigheten – for en behandlingsansvarlig i Danmark: Datatilsynet – før behandlingen dersom en vurdering av personvernkonsekvenser viser at behandlingen vil medføre høy risiko dersom den behandlingsansvarlige ikke treffer tiltak for å redusere risikoen.

9.3 Partene skal i vedlegg C angi de nødvendige tekniske og organisatoriske tiltakene som databehandleren skal bistå den behandlingsansvarlige med, samt i hvilket omfang og hvilken utstrekning. Dette gjelder for de pliktene som følger av bestemmelse 9.1 og 9.2.

10. Varsling om brudd på personopplysningssikkerheten

10.1 Databehandleren underretter uten ugrunnet opphold den behandlingsansvarlige etter å ha blitt oppmerksom på at det har skjedd et brudd på personopplysningssikkerheten.

10.2 Databehandlerens underretning til den behandlingsansvarlige skal om mulig skje senest 24 timer etter at databehandleren har fått kjennskap til bruddet, slik at den behandlingsansvarlige kan overholde sin plikt til å melde bruddet på personopplysningssikkerheten til den kompetente tilsynsmyndigheten, jf. personvernforordningens artikkel 33.

10.3 I samsvar med bestemmelse 9.2.a skal databehandleren bistå den behandlingsansvarlige med å melde bruddet til den kompetente tilsynsmyndigheten. Dette innebærer at databehandleren skal bistå med å fremskaffe informasjonen nedenfor, som i henhold til artikkel 33 nr. 3 skal fremgå av den behandlingsansvarliges melding om bruddet til den kompetente tilsynsmyndigheten:

a) arten av bruddet på personopplysningssikkerheten, herunder, når det er mulig, kategoriene av og omtrentlig antall registrerte som er berørt, og kategoriene av og omtrentlig antall registreringer av personopplysninger som er berørt

b) de sannsynlige konsekvensene av bruddet på personopplysningssikkerheten

c) de tiltakene som den behandlingsansvarlige har truffet eller foreslår å treffe for å håndtere

bruddet på personopplysningssikkerheten, herunder, dersom det er relevant, tiltak for å redusere mulige skadevirkninger som følge av bruddet.

10.4 Partene skal i vedlegg C angi den informasjonen som databehandleren skal fremskaffe i forbindelse med sin bistand til den behandlingsansvarlige med dennes plikt til å melde brudd på personopplysningssikkerheten til den kompetente tilsynsmyndigheten.

11. Sletting og tilbakelevering av opplysninger

11.1 Ved opphør av tjenestene knyttet til behandling av personopplysninger er databehandleren forpliktet til å slette alle personopplysninger som er blitt behandlet på vegne av den behandlingsansvarlige, og bekrefte overfor den behandlingsansvarlige at opplysningene er slettet – med mindre den behandlingsansvarlige senest ved opphøret skriftlig har valgt tilbakelevering, og databehandleren da tilbakeleverer alle personopplysningene og sletter eksisterende kopier – med mindre EU-retten eller medlemsstatenes nasjonale rett krever lagring av personopplysningene. Frist og fremgangsmåte fremgår av vedlegg C.4.

11.2 Ingen regler i EU-retten eller dansk rett krever lagring av de personopplysningene databehandleren behandler på vegne av den behandlingsansvarlige, etter opphør av tjenestene.

12. Revisjon, herunder inspeksjon

12.1 Databehandleren stiller all informasjon som er nødvendig for å påvise overholdelse av personvernforordningens artikkel 28 og disse Bestemmelsene, til rådighet for den behandlingsansvarlige og gir mulighet for og bidrar til revisjoner, herunder inspeksjoner, som utføres av den behandlingsansvarlige eller en annen revisor som er bemyndiget av den behandlingsansvarlige.

12.2 Prosedyrene for den behandlingsansvarliges revisjoner, herunder inspeksjoner, av databehandleren og underdatabehandlere er nærmere angitt i vedlegg C.7 og C.8.

12.3 Databehandleren er forpliktet til å gi tilsynsmyndigheter som etter gjeldende lovgivning har tilgang til den behandlingsansvarliges eller databehandlerens lokaler, eller representanter som opptrer på tilsynsmyndighetens vegne, tilgang til databehandlerens fysiske lokaler mot fremvisning av behørig legitimasjon.

13. Partenes avtale om andre forhold

13.1 Partene kan avtale andre bestemmelser knyttet til tjenesten som gjelder behandling av personopplysninger, om for eksempel erstatningsansvar, så lenge disse andre bestemmelsene ikke direkte eller indirekte strider mot Bestemmelsene eller svekker den registrertes grunnleggende rettigheter og friheter som følger av personvernforordningen.

14. Ikrafttredelse og opphør

14.1 Bestemmelsene trer i kraft på datoen for begge parters underskrift av dem. Underskrift kan skje elektronisk i Svarflows oppsettsprosess (navn, stilling, tidspunkt og avtaleversjon registreres), jf. personvernforordningens artikkel 28 nr. 9.

14.2 Begge parter kan kreve Bestemmelsene reforhandlet dersom lovendringer eller uhensiktsmessigheter i Bestemmelsene gir grunn til det.

14.3 Bestemmelsene gjelder så lenge tjenesten knyttet til behandling av personopplysninger varer. I denne perioden kan Bestemmelsene ikke sies opp, med mindre andre bestemmelser som regulerer leveringen av tjenesten knyttet til behandling av personopplysninger, avtales mellom

partene.

14.4 Dersom leveringen av tjenestene knyttet til behandling av personopplysninger opphører, og personopplysningene er slettet eller tilbakelevert til den behandlingsansvarlige i samsvar med bestemmelse 11.1 og vedlegg C.4, kan Bestemmelsene sies opp med skriftlig varsel av hver av partene.

Underskrift

På vegne av den behandlingsansvarlige

Navn	[Navn]
Stilling	[Stilling]
Telefonnummer	[Telefonnummer]
E-post	[E-post]
Dato og underskrift	

På vegne av databehandleren

Navn	Jesper Rune Thomasen
Stilling	Daglig leder, Svarflow ApS
Telefonnummer	+45 35 15 47 47
E-post	legal@svarflow.dk
Dato og underskrift	

15. Kontaktpersoner hos den behandlingsansvarlige og databehandleren

15.1 Partene kan kontakte hverandre via kontaktpersonene nedenfor.

15.2 Partene er forpliktet til løpende å orientere hverandre om endringer som gjelder kontaktpersoner.

Den behandlingsansvarliges kontaktperson

Navn	[Navn]
Stilling	[Stilling]
Telefonnummer	[Telefonnummer]
E-post	[E-post]

Databehandlerens kontaktperson

Navn	Jesper Rune Thomasen
Stilling	Daglig leder
Telefonnummer	+45 35 15 47 47
E-post	legal@svarflow.dk (henvendelser om personopplysninger, de registrertes rettigheter og sikkerhetshendelser)

Vedlegg A — Opplysninger om behandlingen

A.1. Formålet med databehandlerens behandling av personopplysninger på vegne av den behandlingsansvarlige

Databehandleren besvarer telefonanrop til den behandlingsansvarliges virksomhet med AI-telefonresepsjonisten Nora og utfører på vegne av den behandlingsansvarlige:

- besvarelse av innkommende anrop på den behandlingsansvarliges telefonnummer,
- booking, flytting og avbestilling av avtaler i den behandlingsansvarliges egen kalender eller bookingsystem etter den behandlingsansvarliges regler,
- beskjeder til den behandlingsansvarlige om det innringeren ønsker,
- SMS-bekreftelser til innringeren (innringeren bekrefter selv en avtale før den gjelder),
- viderekobling til den behandlingsansvarliges eget nummer når den behandlingsansvarlige har valgt det.

A.2. Databehandlerens behandling av personopplysninger på vegne av den behandlingsansvarlige gjelder primært (behandlingens art)

Mottak av anropet, omgjøring av tale til tekst, samtale med innringeren ved hjelp av en språkmodell, oppsummering, lagring og videreformidling til den behandlingsansvarlige av samtalens innhold – samt lydopptak dersom den behandlingsansvarlige har valgt det (regelen «Lagre lyd fra samtalene» i Svarflows administrasjonsgrensesnitt; som standard av) – og opprettelse, endring og avbestilling av avtaler i den behandlingsansvarliges kalender.

A.3. Behandlingen omfatter følgende typer personopplysninger om de registrerte

- navn
- telefonnummer
- e-postadresse, dersom innringeren oppgir den
- tidspunkt for anropet og anropets varighet
- samtalens innhold: transkripsjon og sammendrag – og lydopptak dersom den behandlingsansvarlige har valgt det (regelen «Lagre lyd fra samtalene»; som standard av)
- bookingopplysninger: hva avtalen gjelder, når og hos hvem, samt innringerens merknader til avtalen

Sensitive personopplysninger (artikkel 9). Hos behandlingsansvarlige i helsesektoren og lignende kan helseopplysninger forekomme i samtalens innhold, fordi innringeren selv forteller om dem. Nora spør aldri om helseopplysninger, fødselsnumre eller betalingsopplysninger – det er en fast instruks – og dersom innringeren likevel oppgir dem, gjentar og noterer Nora dem ikke. De kan likevel inngå i transkripsjonen av samtalen og i lydopptaket, dersom den behandlingsansvarlige har valgt det. Den behandlingsansvarlige må derfor ta stilling til om behandlingen hos nettopp den behandlingsansvarlige omfatter artikkel 9-opplysninger, og sikre et behandlingsgrunnlag for dem.

A.4. Behandlingen omfatter følgende kategorier av registrerte

Den behandlingsansvarliges kunder, pasienter, klienter eller gjester – det vil si de personene som ringer til den behandlingsansvarliges telefonnummer, og de personene en avtale opprettes for. Dessuten den behandlingsansvarliges ansatte i den grad de opptrer som behandler eller kontaktperson på en avtale.

A.5. Databehandlerens behandling av personopplysninger på vegne av den behandlingsansvarlige kan påbegynnes etter at disse Bestemmelsene har trådt i kraft. Behandlingen har følgende varighet

Behandlingen pågår så lenge abonnementsavtalen om Tjenesten mellom partene er i kraft. Ved opphør slettes eller tilbakeleveres personopplysningene etter den behandlingsansvarliges valg innen 90 dager, jf. bestemmelse 11.1 og vedlegg C.4.

Vedlegg B — Underdatabehandlere

B.1. Godkjente underdatabehandlere

Ved Bestemmelsenes ikrafttredelse har den behandlingsansvarlige godkjent bruken av følgende underdatabehandlere:

Underdatabehandler	Rolle i behandlingen	Land / sted for behandling	Overføringsgrunnlag
Telnyx LLC	Telefoni: mottar anropet på den behandlingsansvarliges nummer og kobler det til Nora	USA	EU-kommisjonens standardpersonvernbestemmelser (2021/914) i Telnyx' databehandleravtale; Telnyx er dessuten sertifisert under EU-U.S. Data Privacy Framework
ElevenLabs, Inc.	Tale til tekst, Noras stemme og samtale-AI; språkmodellen i samtalen kalles via ElevenLabs. Lyd og transkripsjon slettes hos ElevenLabs etter 30 dager	USA	Standardpersonvernbestemmelser (2021/914) i ElevenLabs' databehandleravtale; ElevenLabs er dessuten sertifisert under EU-U.S. Data Privacy Framework
Anthropic, PBC	Språkmodell i samtalen (via ElevenLabs) og analyse av samtaler: sammendrag, beskjed til den behandlingsansvarlige, kvalitetsmåling	USA	Standardpersonvernbestemmelser (2021/914, modul 2 og 3) i Anthropics databehandleravtale. Kundedata brukes ikke til trening av modeller
Vercel Inc.	Drift av Svarflows programvare (serverfunksjoner)	USA; funksjonene kjøres i Frankfurt, Tyskland (region fra1)	Standardpersonvernbestemmelser (2021/914) i Vercels databehandleravtale
Supabase Pte. Ltd	Database, filer (herunder lydopptak) og innlogging	Singapore; databasen og filene ligger i Frankfurt, Tyskland (AWS eu-central-1)	Standardpersonvernbestemmelser (2021/914, modul 2 og 3) i Supabases databehandleravtale
ONLINECITY.IO ApS (GatewayAPI), CVR-nummer 27364276	SMS til de registrerte (bekreftelser og beskjeder)	Danmark; hosting hos Hetzner Online GmbH, Tyskland (EU-oppsett)	Ingen overføring til tredjeland
Simply.com A/S	Utgående e-post til den behandlingsansvarlige (beskjeder og varsler)	Danmark	Ingen overføring til tredjeland
Hetzner Online GmbH	Svarflows integrasjonsserver mot den behandlingsansvarliges bookingsystem (sky-connector)	Tyskland (Falkenstein)	Ingen overføring til tredjeland

Den behandlingsansvarliges egne leverandører. Bruker den behandlingsansvarlige Google Kalender eller et annet bookingsystem, skriver Svarflow avtalene inn i den behandlingsansvarliges egen konto hos den aktuelle leverandøren. Leverandøren behandler da opplysningene under den behandlingsansvarliges egen avtale med leverandøren og er ikke Svarflows underdatabehandler.

Oppsett. Ved oppsettet leser Svarflow den behandlingsansvarliges offentlige nettsted gjennom tjenesten Firecrawl (SideGuide Technologies, Inc., USA) for å bli kjent med virksomhetens tjenester og åpningstider. Det sendes ingen opplysninger om de registrerte til denne tjenesten.

Ved Bestemmelsenes ikrafttredelse har den behandlingsansvarlige godkjent bruken av ovennevnte underdatabehandlere for den beskrevne behandlingsaktiviteten. Databehandleren kan ikke – uten den behandlingsansvarliges skriftlige godkjenning – benytte en underdatabehandler til en annen behandlingsaktivitet enn den beskrevne og avtalte, eller benytte en annen underdatabehandler til denne behandlingsaktiviteten.

B.2. Varsel for godkjenning av underdatabehandlere

Databehandleren underretter den behandlingsansvarlige skriftlig (per e-post til den behandlingsansvarliges kontaktperson) med minst 30 dagers varsel før en underdatabehandler legges til eller skiftes ut. Den behandlingsansvarlige kan protestere før varselfristen utløper. Kan partene ikke bli enige om protesten, kan den behandlingsansvarlige si opp Tjenesten med virkning fra det tidspunktet den nye underdatabehandleren tas i bruk. Den til enhver tid gjeldende listen over underdatabehandlere finnes på svarflow.dk.

Vedlegg C — Instruks om behandling av personopplysninger

C.1. Behandlingens gjenstand/instruks

Databehandlerens behandling av personopplysninger på vegne av den behandlingsansvarlige skjer ved at databehandleren utfører følgende:

- besvarer anrop til den behandlingsansvarliges nummer med AI-telefonresepsjonisten Nora,
- oppretter, flytter og avbestiller avtaler i den behandlingsansvarliges kalender eller bookingsystem etter den behandlingsansvarliges bookingregler – en avtale gjelder først når innringeren selv har bekreftet den via SMS,
- tar imot beskjeder til den behandlingsansvarlige og videreformidler dem per e-post, SMS eller i Svarflows administrasjonsgrensesnitt,
- sender SMS-bekreftelser til innringeren,
- oppgir den behandlingsansvarliges eget vaktnummer eller kobler videre etter den behandlingsansvarliges instruks.

Den behandlingsansvarlige styrer selv reglene – åpningstider, bookingregler, hilsen, instruks for akutte henvendelser, om det kan tas opp lyd, hvor lenge samtaler lagres, og når Nora skal ta imot en beskjed – i Svarflows administrasjonsgrensesnitt. Endringer her er dokumenterte instrukser, jf. bestemmelse 4.1.

Nora gir ikke helsefaglig rådgivning, vurderer ikke symptomer og treffer ingen avgjørelser om den registrerte. Nora opplyser i hilsenen at innringeren snakker med en AI-assistent.

Lydopptak skjer bare når den behandlingsansvarlige har valgt det (regelen «Lagre lyd fra samtalene»), for å dokumentere hva som ble sagt og avtalt – transkripsjonen kan være feil, og behovet kan derfor ikke dekkes på annen måte (det danske Datatilsynets veiledning om opptak av telefonsamtaler, april 2024). Innringeren informeres i hilsenen om opptaket og formålet.

C.2. Behandlingssikkerhet

Sikkerhetsnivået skal gjenspeile:

- at det behandles alminnelige personopplysninger om de registrerte (navn, telefonnummer, samtaleinnhold og avtaler),
- at helseopplysninger kan forekomme i samtalens innhold hos behandlingsansvarlige i

helsesektoren, fordi innringeren selv forteller om dem (vedlegg A.3), og
- at samtalens innhold behandles i klartekst hos underdatabehandlere i USA, for at Nora skal kunne forstå og svare (vedlegg C.6).

Databehandleren er deretter berettiget og forpliktet til å treffe beslutninger om hvilke tekniske og organisatoriske sikkerhetstiltak som skal gjennomføres for å etablere det nødvendige (og avtalte) sikkerhetsnivået.

Databehandleren skal likevel – under alle omstendigheter og som et minimum – gjennomføre følgende tiltak, som er avtalt med den behandlingsansvarlige:

- Kryptering under overføring: all kommunikasjon mellom Svarflows programvare, de registrerte og underdatabehandlerne skjer over TLS.
- Kryptering ved lagring: data krypteres ved lagring hos underdatabehandlerne (database, filer og lydopptak).
- Den behandlingsansvarliges innlogging i bookingsystemet: når Svarflow kobler seg til den behandlingsansvarliges bookingsystem med den behandlingsansvarliges egen tilgang, krypteres innloggingsopplysningene med en nøkkel som bare integrasjonsserveren i EU kan åpne (X25519 og AES-256-GCM). Verken Svarflows serverfunksjoner eller databasen kan lese dem, og de slettes når den behandlingsansvarlige kobler fra forbindelsen.
- Nøkkelhåndtering: produksjonsnøkler ligger utelukkende i kryptert miljøkonfigurasjon hos driftsleverandøren og deles aldri i klartekst, i kildekode eller i loggfiler.
- Tilgangsstyring: tilgang til Svarflows administrasjonsgrensesnitt krever personlig innlogging; funksjoner for Svarflows ansatte er låst til godkjente kontoer. Listen over personer med tilgang gjennomgås løpende, jf. bestemmelse 5.1.
- Tilgang via internett: den behandlingsansvarliges tilgang til egne opplysninger skjer over TLS etter personlig innlogging; databasen tillater bare de lesingene og skrivingene den enkelte rollen har rett til (radbasert tilgangskontroll).
- Endringskontroll: hver endring i systemet testes av automatiske testlåser, som alle må være grønne før en endring kan rulles ut.
- Logging: driftslogger inneholder korte id-er, tidsstempler og maskerte telefonnumre – ikke samtaleinnhold eller fullstendige personopplysninger.
- Dataminimering ved kilden: Noras instruks tillater bare å be om det oppgaven krever – typisk navn og mobilnummer – og forbyr å be om fødselsnummer, betalingskort, kontonumre, passord og helsedetaljer.
- Bekreftelse fra den registrerte: ingenting Nora avtaler, skrives inn i den behandlingsansvarliges kalender før innringeren selv har bekreftet det via en lenke i en SMS. Lenken utløper etter 24 timer.
- Begrenset lagring hos underdatabehandler: ElevenLabs lagrer lyd og transkripsjon i 30 dager, og deretter slettes de. Lyd tas bare opp når den behandlingsansvarlige har valgt det.
- Feilskjermbilder fra integrasjonsserveren: tas aldri på innloggingstrinnet, lagres med begrensede rettigheter uten personopplysninger i filnavnet og slettes automatisk etter 72 timer.
- Atskillelse av test og produksjon: testdata opprettes aldri med ekte identitetsopplysninger.
- Regelmessig testing: sikkerhetstiltakene gjennomgås minst én gang årlig og ved vesentlige endringer i systemet eller hos underdatabehandlerne; gjennomgangen dokumenteres.

Tiltakene er de faktisk gjennomførte. Databehandleren er ikke ISO 27001-sertifisert, har ikke en SOC 2-erklæring og har ikke fått gjennomført en ekstern sikkerhetstest av tredjepart. Dette opplyses åpent, slik at den behandlingsansvarlige kan vurdere om ytterligere tiltak skal avtales, jf. bestemmelse 6.4.

C.3. Bistand til den behandlingsansvarlige

Databehandleren skal så langt det er mulig – innenfor det omfanget og den utstrekningen som er angitt nedenfor – bistå den behandlingsansvarlige i samsvar med bestemmelse 9.1 og 9.2 ved å gjennomføre følgende tekniske og organisatoriske tiltak:

- De registrertes rettigheter (artikkel 15–22): databehandleren finner frem og utleverer de opplysningene som er behandlet om en registrert (samtaler, avtaler og beskjeder), og sletter eller retter dem etter den behandlingsansvarliges instruks. Anmodninger sendes til legal@svarflow.dk og besvares senest 10 virkedager etter mottak, slik at den behandlingsansvarlige kan overholde sin egen frist på én måned.
- Behandlingssikkerhet (artikkel 32): ved å opprettholde tiltakene i C.2 og opplyse om dem på anmodning.
- Brudd på personopplysningssikkerheten (artikkel 33–34): ved å underrette den behandlingsansvarlige innen fristen i bestemmelse 10.2 og fremskaffe opplysningene i bestemmelse 10.3: hendelsens art, tidspunktet for hendelsen og for når den ble oppdaget, de berørte opplysningstypene og omtrentlig antall berørte registrerte, de sannsynlige konsekvensene, de tiltakene databehandleren har truffet, og databehandlerens anbefaling om melding og underretning. Underretningen sendes per e-post til den behandlingsansvarliges kontaktperson og følges opp etter hvert som databehandleren vet mer.
- Vurdering av personvernkonsekvenser og forhåndsdrøftinger (artikkel 35–36): databehandleren stiller dette vedlegget, listen over underdatabehandlere, overføringsvurderingen og annen nødvendig dokumentasjon til rådighet.

C.4. Lagringsperiode/sletterutine

Opplysninger	Lagring og sletting
Personopplysninger på en booking (ordrekøen)	Viskes ut automatisk når ordren er gjennomført
Ventekort (avtale som venter på innringerens bekreftelse)	Utløper etter 24 timer uten bekreftelse; viskes ut automatisk senest etter 7 dager
Transkripsjon og sammendrag	Den behandlingsansvarliges valg: 30, 90 (standard) eller 180 dager
Lydopptak (bare ved «Lagre lyd fra samtalene» – den behandlingsansvarliges valg, som standard av)	Den behandlingsansvarliges valg: 30, 90 (standard) eller 180 dager
Lyd og transkripsjon hos ElevenLabs (underdatabehandler)	Slettes automatisk etter 30 dager
Beskjeder til den behandlingsansvarlige	Så lenge abonnementet løper; slettes ved opphør som angitt nedenfor
Ved avtalens opphør	Alle personopplysninger slettes eller tilbakeleveres etter den behandlingsansvarliges valg innen 90 dager, og deretter bekrefter databehandleren slettingen skriftlig

Fristene for ordrekøen, ventekort, transkripsjon, sammendrag og lydopptak håndheves automatisk av systemet: en daglig jobb visker personopplysningene ut av samtalen, sletter lydfilen og etterlater bare det driften trenger (samtale-id, varighet og utfall). Den behandlingsansvarlige velger selv fristen – 30, 90 eller 180 dager – i Svarflows administrasjonsgrensesnitt; velges en kortere frist, viskes eldre samtaler ut ved neste nattlige kjøring. Sletting ved avtalens opphør utføres av databehandleren etter

den behandlingsansvarliges valg, jf. bestemmelse 11.1.

Ved opphør av tjenesten knyttet til behandling av personopplysninger skal databehandleren enten slette eller tilbakelevere personopplysningene i samsvar med bestemmelse 11.1, med mindre den behandlingsansvarlige – etter underskriften av disse Bestemmelsene – har endret den behandlingsansvarliges opprinnelige valg. Slike endringer skal være dokumentert og oppbevares skriftlig, herunder elektronisk, i tilknytning til Bestemmelsene.

C.5. Sted for behandling

Behandling av personopplysningene som omfattes av Bestemmelsene, kan ikke uten den behandlingsansvarliges forutgående skriftlige godkjenning skje på andre steder enn følgende:

- Frankfurt, Tyskland (EU): Svarflows egen programvare (Vercel, region fra1) og databasen med filer og lydopptak (Supabase, AWS eu-central-1).
- Falkenstein, Tyskland (EU): Svarflows integrasjonsserver (Hetzner) og hostingen av SMS-utsendelsen (GatewayAPI).
- Danmark: utgående e-post (Simply.com).
- USA: telefoni (Telnyx), tale til tekst, stemme og samtale-AI (ElevenLabs) samt språkmodell og analyse av samtaler (Anthropic).
- Singapore: Supabases kontraktspart; selve databasen ligger i Frankfurt.

C.6. Instruks om overføring av personopplysninger til tredjeland

Den behandlingsansvarlige instruerer databehandleren om å overføre personopplysninger til de underdatabehandlerne i USA og Singapore som fremgår av vedlegg B, på det overføringsgrunnlaget som er angitt for hver enkelt: EU-kommisjonens standardpersonvernbestemmelser (gjennomføringsbeslutning (EU) 2021/914, personvernforordningens artikkel 46 nr. 2 bokstav c), som inngår i hver leverandørs databehandleravtale. Der leverandøren dessuten er sertifisert under EU-U.S. Data Privacy Framework, hviler overføringen også på EU-kommisjonens beslutning om tilstrekkelig beskyttelsesnivå av 10. juli 2023 (artikkel 45); standardpersonvernbestemmelsene gjelder uansett.

Overføringen er nødvendig for å levere Tjenesten: samtalen må behandles i klartekst for at Nora skal kunne forstå og svare, og det fjernes ingen opplysninger før overføringen. Databehandleren har vurdert overføringene (overføringsvurdering) og stiller vurderingen til rådighet for den behandlingsansvarlige på anmodning. Databehandleren reviderer overføringsgrunnlaget dersom beslutningen om tilstrekkelig beskyttelsesnivå oppheves eller suspenderes, og underretter den behandlingsansvarlige dersom det endrer grunnlaget for en underdatabehandler.

Dersom den behandlingsansvarlige ikke i disse Bestemmelsene eller senere gir en dokumentert instruks om overføring av personopplysninger til et tredjeland, er databehandleren ikke berettiget til innenfor rammene av disse Bestemmelsene å foreta slike overføringer.

C.7. Prosedyrer for den behandlingsansvarliges revisjoner, herunder inspeksjoner, av behandlingen av personopplysninger som er overlatt til databehandleren

Den behandlingsansvarlige eller en representant for den behandlingsansvarlige kan én gang årlig – og i tillegg dersom det har skjedd et brudd på personopplysningssikkerheten, eller en tilsynsmyndighet krever det – foreta en revisjon, herunder inspeksjon, av databehandlerens behandling av personopplysninger. Revisjonen varsles skriftlig minst 30 dager i forveien, med mindre den skyldes et brudd. Databehandleren stiller den nødvendige dokumentasjonen til rådighet: dette vedlegget, listen over underdatabehandlere og deres databehandleravtaler (jf. bestemmelse 7.5), beskrivelsen av de tekniske og organisatoriske tiltakene i C.2, overføringsvurderingen, prosedyren for håndtering av brudd på personopplysningssikkerheten og protokollen over behandlingsaktiviteter.

Databehandleren innhenter ikke revisjonserklæringer fra uavhengig tredjepart (f.eks. ISAE 3000). Den

behandlingsansvarliges eventuelle kostnader i forbindelse med en revisjon dekkes av den behandlingsansvarlige selv. Databehandleren er likevel forpliktet til å avsette de ressursene (hovedsakelig den tiden) som er nødvendige for at den behandlingsansvarlige skal kunne gjennomføre sin revisjon. Basert på resultatene er den behandlingsansvarlige berettiget til å anmode om gjennomføring av ytterligere tiltak for å sikre overholdelse av personvernforordningen og disse Bestemmelsene.

C.8. Prosedyrer for revisjoner, herunder inspeksjoner, av behandling av personopplysninger som er overlatt til underdatabehandlere

Underdatabehandlerne dokumenterer sin sikkerhet gjennom uavhengige revisjonsrapporter og sertifiseringer (f.eks. SOC 2, ISO 27001 eller ISAE 3000). Databehandleren innhenter og gjennomgår dem minst én gang årlig og under alle omstendigheter dersom en underdatabehandler endrer sin behandling vesentlig eller rammes av et brudd. Dokumentasjonen stilles til rådighet for den behandlingsansvarlige på anmodning. Databehandleren foretar ikke fysiske inspeksjoner hos underdatabehandlerne. Basert på resultatene er den behandlingsansvarlige berettiget til å anmode om gjennomføring av ytterligere tiltak, og den behandlingsansvarlige kan protestere mot en underdatabehandler etter vedlegg B.2.

Vedlegg D — Partenes regulering av andre forhold

Partenes avtale om erstatningsansvar følger abonnementsavtalen om Tjenesten, i den grad den ikke direkte eller indirekte strider mot Bestemmelsene eller svekker de registrertes rettigheter, jf. bestemmelse 13.1. Utover dette har partene ikke avtalt særskilte bestemmelser.

Dokumentet bygger på det danske Datatilsynets standardkontraktsbestemmelser (januar 2020), som Det europeiske personvernrådet har avgitt uttalelse om (uttalelse 14/2019). Bestemmelsene 2–15 er standardavtalens tekst med partenes valg utfylt; vedlegg A–D er Svarflows. Ved motstrid mellom en oversettelse og den danske teksten gjelder den danske.