Databehandleravtale

Denne databehandleravtale er inngått mellom:

Fyll inn firmanavn og org.nr **(«Behandlingsansvarlig»)**

og

Exsitec AS, org.nr. 984489234, Nye Vakåsvei 64, 1395 Hvalstad **(“Databehandler”).**

1. Bakgrunn

Den behandlingsansvarlige og databehandleren har inngått en eller flere avtaler om implementering, tilpasning og utvikling av standard IT-løsning, brukerstøtte, konsulenttjenester eller forvalting, heretter benevnt som tjenesteavtalen. Se vedlegg 1.

I forbindelse med databehandlerens leveranser etter tjenesteavtalen vil databehandleren behandle personopplysninger på vegne av den behandlingsansvarlige.

2. Definisjoner

Disse begrepene skal forstås som følger:

Avtalen: Denne databehandleravtalen med vedlegg.

Tjenesteavtale: Den avtalen som det henvises til i pkt. 1. Ved ev. motstrid mellom databehandleravtalen og tjenesteavtalen går databehandleravtalen foran tjenesteavtalen når det gjelder behandlingen av personopplysninger.

Personopplysninger: De personopplysninger som databehandleren behandler på vegne av den behandlingsansvarlige i henhold til denne avtalen. Dette kan være alle typer informasjon som direkte eller indirekte kan knyttes til en fysisk person, og som behandles på vegne av den behandlingsansvarlige.

Behandlingsansvarlig: Det rettssubjekt som bestemmer formålet med behandlingen av personopplysningene og hvilke midler som skal benyttes.

Databehandler: Det rettssubjekt som behandler personopplysningene på vegne av den behandlingsansvarlige i henhold til denne avtalen.

Underdatabehandler: Underleverandører som behandler personopplysninger på vegne av databehandleren.

Tredjepart: Leverandører som den behandlingsansvarlige har engasjert som databehandler skal samarbeide med og kan utlevere/overføre personopplysninger til.

Registrert: Den fysiske personen som personopplysningene kan knyttes til.

Personvernlovgivning: De til enhver tid gjeldende lover og forskrifter om behandling av personopplysninger, tilsynsmyndighetenes avgjørelser og retningslinjer, samt foreliggende rettspraksis.

Personvernforordningen (GDPR): Forordning (EU) 2016/679 av Europaparlamentet og Rådet av 27.04.2016 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.

Tilsynsmyndighet: Den eller de tilsynsmyndigheter som har myndighet til å føre tilsyn med behandling av personopplysninger som er underlagt personvernlovgivningen, i Norge Datatilsynet.

3. Behandling av personopplysninger

3.1 Databehandleren skal bare behandle personopplysninger i henhold til de til enhver tid gjeldende dokumenterte instruksjoner fra den behandlingsansvarlige og kun i den utstrekning det er nødvendig for å oppfylle tjenesteavtalen og denne avtale. Databehandleren skal ikke behandle personopplysningene for andre formål enn de som er instruert av den behandlingsansvarlige.

Den behandlingsansvarliges instruksjoner til databehandleren på tidspunktet for avtaleinngåelse, herunder hensikten med behandlingen, behandlingens formål/art, kategorier av registrerte og kategorier/typen personopplysninger, bestemmelser om ev. overføring og retten til å engasjere underdatabehandlere, bruk av tredjeparter mv, fremgår av vedlegg 1.

Vedlegget vil bli oppdatert av den behandlingsansvarlige ved behov, og skal varsles databehandler iht. pkt. 12. Dersom en endring medføre økte kostnader, skal databehandler varsle behandlingsansvarlige om dette innen rimelig tid.

3.2 Dersom databehandleren anser instruksjonene for å være utilstrekkelige for oppfyllelsen av tjenesteavtalen eller for oppfyllelsen av denne avtalen eller krenker personvernlovgivningen, skal databehandleren omgående underrette den behandlingsansvarlige.

3.3 Databehandleren skal uten opphold informere den behandlingsansvarlige om enhver henvendelse fra registrerte, tredjeparter, tilsynsmyndighetene eller annen offentlig myndighet som refererer seg til, eller som kan være av betydning for behandlingen av personopplysningene.

Databehandleren skal ikke representere den behandlingsansvarlige eller handle på dennes vegne uten skriftlig forhåndstillatelse fra den behandlingsansvarlige, jf. pkt. 4.

Dersom databehandleren i henhold til gjeldende lover og forskrifter er pålagt å fremlegge personopplysninger som databehandleren behandler på vegne av den behandlingsansvarlige til tilsynsmyndighetene, annen offentlig myndigheter eller andre,

skal databehandleren øyeblikkelig informere den behandlingsansvarlige om dette, så fremt til er lovlig.

3.4 Databehandleren skal ha rutiner for å registrere avvik fra personopplysningssikkerheten. Databehandleren skal varsle den behandlingsansvarlige om ethvert sikkerhetsbrudd fra personopplysningssikkerheten senest 24 timer etter at sikkerhetsbruddet ble kjent.

I slike tilfeller skal databehandleren

(i) Fremlegge alle detaljer om sikkerhetsbruddet fra personopplysningssikkerheten for den behandlingsansvarlige.

(ii) Etter avtale med den behandlingsansvarlige, iverksette hensiktsmessige tiltak som er nødvendige for å minimere konsekvensene av sikkerhetsbruddet og beskytte mot et tilsvarende fremtidig sikkerhetsbrudd.

(iii) Så tidlig som praktisk mulig etter et sikkerhetsbrudd, informere den behandlingsansvarlige om databehandlerens forslag til tiltak for å forhindre et fremtidig lignende sikkerhetsbrudd.

Den behandlingsansvarlige har ansvaret for at nødvendige avviksmeldinger sendes Datatilsynet og de registrerte.

3.5 Databehandler skal føre påkrevet protokoll over behandlingen av personopplysninger etter denne avtalen i henhold til personvernforordningen (GDPR) art. 30.2 a) - d) og iverksette påkrevde tiltak iht. art. 32.

3.6 Databehandleren skal overholde personvernlovgivning og gjeldende tilrådninger fra tilsynsmyndighetene og annen kompetent myndighet, og til holde seg oppdatert på personvernlovgivningen. Databehandleren skal akseptere å innta enhver endring og ethvert tillegg i denne avtalen som er påkrevd etter personvernlovgivningen.

4. Bistand til behandlingsansvarlig

4.1 Databehandler skal på anmodning fra den behandlingsansvarlige bistå den behandlingsansvarlige med følgende:

- Sikre at den behandlingsansvarlige oppfyller kravene i personvernforordningen (GDPR) art. 32-36.

- Sikre at den behandlingsansvarlige oppfylle plikten til å svare på anmodninger fra den registrerte med henblikk på å utøve rettigheter fastsatt i personvernforordningen (GDPR) art. 16-20.

- Vurdere personvernkonsekvenser og delta i eventuelle forhåndsdrøftelse med tilsynsmyndighetene, jf. personvernforordningen (GDPR) art. 35-36.

4.2 Omfanget avgrenses av behandlingsformen og hvilken informasjon som er tilgjengelig for databehandleren.

Arbeid og kostnader i forbindelse med slik bistand skal kompenseres av den behandlingsansvarlige.

5. Tekniske og organisatoriske tiltak

5.1 Databehandleren er forpliktet til å iverksette alle tiltak som er nødvendig iht. Personvernforordningen (GDPR) art. 32. Tiltakene skal resultere i et sikkerhetsnivå som er hensiktsmessig hensett til eksisterende tekniske muligheter, kostnadene ved å iverksette tiltakene, særlig risiko i tilknytning til behandlingen av personopplysninger og sensitiviteten til personopplysningene som blir behandlet.

Dette omfatter hensiktsmessige tekniske og organisatoriske tiltak for å beskytte personopplysningene mot sletting, endringer, urettmessig overføring, spredning og sikre tilgang. Databehandleren skal også sørge for at personer som er autorisert til å behandle personopplysningene har forpliktet seg til å behandle personopplysningene fortrolig.

5.2 Databehandleren forplikter seg til ikke å legge frem eller på annen måte gjøre personopplysninger tilgjengelig for noen tredjepart, uten skriftlig forhåndstillatelse fra den behandlingsansvarlige. Dette omfatter også å besvare forespørsler fra registrerte.

Unntak gjelder for bindende pålegg fra tilsynsmyndighetene, annen offentlig myndigheter eller andre, samt godkjente underdatabehandlere, jf. pkt. 3.3 og 8.

6. Dokumentasjon og revisjonsrettigheter

Databehandleren skal, etter rimelig varsel, gjøre tilgjengelig for den behandlingsansvarlige eller en utpekt tredjepart all dokumentasjon som er nødvendig for å påvise at forpliktelsene i personvernforordningen (GDPR) art. 28 er oppfylt. Innsyn i dokumentasjonen skal reguleres strengt, og kun gis til et begrenset antall personer som har behov for konkret innsyn for å utføre sine oppgaver, slik at dette ikke svekker sikkerheten.

Behandlingsansvarlige har rett til å la en utpekt tredjepart revidere Databehandlers personopplysningssikkerhet, og/eller utføre stikkprøvekontroller.

Arbeid og kostnader i forbindelse med krav om dokumentasjon og revisjon skal kompenseres av den behandlingsansvarlige.

7. OVERFØRING TIL TREDJELAND

7.1 Databehandleren kan ikke, uten skriftlig forhåndstillatelse fra den behandlingsansvarlige, overføre personopplysninger til land utenfor EU/EØS. Dersom personopplysningene skal overføres til land utenfor EU/EØS, må dette dessuten foreligge et overføringsgrunnlag. For så vidt gjelder bruk av underdatabehandlere, se pkt. 8.

7.2 Den behandlingsansvarlige er berettiget til å trekke tilbake tillatelse til overføringer til tredjeland. I et slikt tilfelle skal databehandleren øyeblikkelig avslutte overføringene og skal, på den behandlingsansvarliges forespørsel, fremlegge skriftlig dokumentasjon på dette.

8. Underdatabehandlere og tredjeparter

8.1 Databehandleren kan ikke engasjere underdatabehandlere til å behandle personopplysninger med mindre den behandlingsansvarlige har gitt særlig eller generell skriftlig tillatelse til dette, jf. vedlegg 1.

Personopplysninger kan utelukkende behandles av en underdatabehandler på betingelse av at databehandleren inngår en skriftlig avtale med denne hvor de samme forpliktelsene som fremgår av denne avtalen med hensyn til vern av personopplysninger pålegges underdatabehandleren. Ved overføring utenfor EU/EØS, skal databehandler i tillegg påse at det foreligger overføringsgrunnlag.

Databehandleren er forpliktet til å informere den behandlingsansvarlige om eventuelle planer om å benytte andre underdatabehandlere eller å skifte ut underdatabehandler, og gi den behandlingsansvarlige muligheten til å motsette seg slike endringer.

Databehandleren er fullt ut ansvarlig overfor den behandlingsansvarlige for utførelsen av underdatabehandlerens forpliktelser.

8.2 Dersom behandlingsansvarliges har engasjert andre leverandører som databehandler skal samarbeide og utlevere/overføre personopplysninger til, skal dette angis som tredjeparter i vedlegg 1.

Behandlingsansvarlige er fullt ut ansvarlig overfor databehandleren for utførelsen av tredjeparts forpliktelser, samt å sørge for overføringsgrunnlag og databehandleravtale med tredjepart.

9. Ikraftsettelse, oppsigelse og opphør

9.1 Denne avtalen trer i kraft ved signering av begge parter og skal gjelder så lenge databehandleren behandler personopplysninger på vegne av den behandlingsansvarlige.

Den behandlingsansvarlige kan når som helst si opp avtalen med virkning fra den datoen den behandlingsansvarlige fastsetter. De økonomiske virkningene av en oppsigelse av avtalen følger av bestemmelsene i tjenesteavtalen.

9.2 I forbindelse med opphør av avtalen eller tjenesteavtalen, skal databehandleren slette eller tilbakelevere alle personopplysninger til den behandlingsansvarlige, etter den behandlingsansvarliges valg, og slette alle eksisterende kopier, med mindre personvernlovgivingen eller annet gjeldende regelverk tilsier at personopplysningene lagres.

Arbeid og kostnader i den forbindelse skal kompenseres av den behandlingsansvarlige.

10. Vederlag

Når avtalen fastsetter at arbeid og/eller kostnader skal kompenseres av den behandlingsansvarlige, skal dette kompenseres i henhold til medgått tid etter de timesatser som fremgår av tjenesteavtalen. I tillegg kommer kostnader og ev. utlegg iht. statens satser.

Alternativt kan partene enes om annen betalingsmodell.

Vederlaget faktureres i utgangspunktet måneden etter at det er påløpt, med 14 dagers forfall med mindre det fremgår noe annet av tjenesteavtalen eller konkret avtale.

11. Ansvar

Databehandler er ansvarlig for direkte tap som skyldes databehandlers behandling av personopplysninger forutsatt at databehandler ikke har oppfylt forpliktelser i personvernforordning (GDPR) som særlig er rettet mot databehandlere og som ikke kan avvikes ved avtale med behandlingsansvarlige, eller dersom databehandler har opptrådt utenfor eller i strid med behandlingsansvarliges lovlige instrukser.

Erstatning for indirekte tap kan ikke kreves. Indirekte tap omfatter, men er ikke begrenset til, tapt fortjeneste av enhver art, tapte besparelser, tap av data og krav fra tredjeparter.

Samlet erstatning er begrenset til et beløp som tilsvarer kontraktssummen (ekskl. merverdiavgift) iht. tjenesteavtalen og denne avtale.

Dersom databehandler har måttet betale erstatning for skade etter krav fra registrerte, skal databehandler ha regressrett mot den behandlingsansvarlige for den delen av erstatningen som svarer til den behandlingsansvarlige del av ansvaret for skaden, jf. personvernforordningen (GDPR) art. 82.

De samme ansvarsbegrensninger som gjelder etter tjenesteavtalen gjelder også for ansvar iht. denne databehandleravtale.

12. Varsler

12.1 Ethvert varsel som i henhold til avtalen er pålagt å være skriftlig, skal sendes til partenes representant som oppgitt i vedlegg 1, eller til det de senere er endret til. Innholdet i varselet avgjør oversendelsesform, dvs. overlevering, oversendelse pr. post eller e-post.

12.2 Varsel skal anses for å være mottatt av en part:

a) hvis det er leveres av bud: ved leveranse;

b) hvis det sendes med rekommandert brev: to virkedager etter postlegging;

c) hvis det er sendt per e-post: på tidspunktet for sending, dersom mottakelse bekreftes av den mottagende parten.

13. Overdragelse

Ingen av partene skal overdra sine rettigheter og/eller forpliktelser etter denne avtalen uten skriftlig forhåndssamtykke fra den andre parten.

14. Tvister

Partenes rettigheter og plikter etter denne avtalen bestemmes i sin helhet av norsk rett.

Dersom det oppstår uenighet mellom partene om tolkning eller rettsvirkninger av avtalen, skal partene først forsøke å bli enige gjennom forhandlinger.

Dersom en tvist ikke blir løst ved forhandlinger, kan hver av partene forlange tvisten avgjort med endelig virkning ved norske domstoler. Databehandlers hjemting er avtalt verneting.

Partene kan alternativt avtale at tvisten blir avgjort med endelig virkning ved voldgift.

Denne avtalen er inngått i to eksemplar, ett til hver av partene.

Kunde

Fyll inn firmanavn,

adresse og

Org nr. her

Sted/Dato:

Underskrift
Kundens signatur

Leverandør

Exsitec AS
Nye Vakåsvei 64
1395 Hvalstad
Org.nr: 984489234

Sted/Dato: Hvalstad/Dato

Underskrift
Asle Sjørbotten, daglig leder

Avtale godkjennes via Visma Sign (elektronisk signering)

Vedlegg 1:

Instruksjoner og nærmere opplysninger om behandlingen

Den behandlingsansvarliges instruksjoner til databehandleren på tidspunktet for avtaleinngåelse, herunder hensikten med behandlingen, behandlingens formål/art, kategorier av registrerte og kategorier/typen personopplysninger, bestemmelser om ev. overføring og retten til å engasjere underdatabehandlere, bruk av tredjeparter mv, fremgår nedenfor.

Vedlegget vil kunne endres av den behandlingsansvarlige etter varsel til databehandler, jf. avtalen pkt. 3.1 og 12.

Tjenesteavtale Spesifiser hvilken tjenesteavtale som partene har inngått og som er grunnlaget for databehandlers behandlingen av personopplysninger:	**{name}** har avtale med **Exsitec AS** om brukerstøtte for **aktive produkter støttet av Exsitec.** Ved konsulentoppdrag, utvikling, e.l., henvises det til oppdragsbeskrivelser.
Varsler Spesifiser adressat og kontaktopplysninger for skriftlige varsler:	Behandlingsansvarlig: Kontaktperson: Postadresse: E-post: Databehandler: Daglig leder Postadresse: Nye Vakåsvei 64, 1395 Hvalstad E-post: kundesenter@exsitec.no
Hensikt og formål/art Spesifiser hensikten og formålet med databehandlerens behandling av personopplysningene:	Å oppfylle tjenesteavtalen og avtalen
Kategorier av registrerte Spesifiser hvilke kategorier av registrerte personopplysningene som databehandleren skal behandle knytter seg til:	Den behandlingsansvarliges kunder, deres sluttkunder, leverandører og ansatte.
Kategorier/typen personopplysninger Spesifiser hvilke kategorier/type personopplysninger som databehandleren skal behandle:	Fornavn ☐ Etternavn ☐ Direkte telefonnummer ☐ Mobilnummer ☐ E-postadresse ☐ Interesser ☐ Lønnsinformasjon ☐ Kontonummer ☐ Fødselsnummer ☐ Annet :

Kategorier av sensitive/særlige personopplysninger * Spesifiser hvilke sensitive/særlige kategorier av personopplysninger[1] som databehandleren skal behandle:	Sett inn nærmere informasjon
Behandlingsaktiviteter Spesifiser hvilke behandlingsaktiviteter som skal utføres av databehandleren:	F.eks. registrering, organisering, strukturering, lagring, gjenfinning, konsultering, overføring, sammenstilling og sletting
Tekniske og organisatoriske sikkerhetskrav Spesifiser ev. tekniske og organisatoriske sikkerhetstiltak som databehandleren skal iverksette:	I henhold til Exsitec AS sin sikkerhetsinstruks hvis ikke annet er nevnt. <åpent for endringer>
Oppbevaringstid/sletting Spesifiser ev. bestemmelser/krav til oppbevaringstid/sletting for personopplysninger som databehandleren skal lagre:	Sett ev. inn nærmere informasjon <åpent for endringer>
Overføring til land utenfor EU/EØS Spesifiser ev. tillatelse til å overføre personopplysninger til land utenfor EU/EØS: Dette omfatter hvor de ansatte som skal behandle opplysningene er lokalisert.	Ved avtaleinngåelse foreligger det ingen tillatelse til overføring til land utenfor EU/EØS.
Underdatabehandlere Spesifiser ev. tillatelse til å engasjere underdatabehandlere, med angivelse av lokasjon (innenfor EU/EØS eller utenfor med angivelse av land, og ev. krav til overføringsgrunnlag): Men lokasjon menes både der underdatabehandler er lokalisert og der underdatabehandlerens ansatte som skal behandle opplysningene er lokalisert.	Den behandlingsansvarlige tillater databehandleren å benytte underdatabehandlere innenfor EØS/EU under forutsetning av at databehandleren til enhver tid har en oppdatert liste (se under) over de underdatabehandlere som benyttes med angivelse av lokasjon, og varsler den behandlingsansvarlige om planlagte endring og gir den behandlingsansvarlige mulighet til å protestere. Se underdatabehandlere her.
Tredjeparter Spesifiser hvilke tredjeparter som den behandlingsansvarlige har engasjert som databehandler skal samarbeide med og kan utlevere/overføre personopplysninger til:	Sett ev. inn nærmere informasjon <åpent for endringer>

[1]* Sensitive/særlige kategorier av personopplysninger er personopplysninger om rasemessig eller etnisk opprinnelse, politisk oppfatning, religion, overbevisning eller fagforeningsmedlemskap, samt behandling av genetiske opplysninger og biometriske opplysninger med det formål å entydig identifisere en fysisk person, helseopplysninger eller opplysninger om en fysisk persons seksuelle forhold eller seksuelle orientering