# Lisensavtale for Sticos Personal

1. **Avtalens omfang**

   Denne avtalen mellom Sticos AS (org.nr. 934 228 391) og Kunden gir kunden rett til bruk av produktet Sticos Personal i avtaleperioden for det oppgitte antall ansatte i de virksomheter som omfattes av avtalen. Om ikke annet er avtalt løper avtaleperioden i 12 måneder, første gang fra det tidspunktet hvor produktet etter abonnementsavtalen første gang gjøres tilgjengelig for kunden og ellers fra tidspunktet for siste fornyelse av tidligere inngått avtale. Avtaleperioden fornyes automatisk i samsvar med bestemmelsene i punkt 13.

   Bruk av Sticos Personal skal til enhver tid skje i henhold til de betingelser som fremgår av denne avtalen, samt opplysninger oppgitt i tilbud og kundens bestilling.

   Partene kan ikke overdra sine rettigheter og plikter etter denne avtalen uten skriftlig samtykke fra den andre parten. Samtykke kan ikke nektes uten saklig grunn.

2. **Produktet**

   Sticos Personal er et web-basert HMS- og personalverktøy som består av fire ulike moduler:

   a) Personalhåndbok

   b) Lederhåndbok

   c) HMS-verktøy

   d) HR-system

   Til enhver tid oppdatert informasjon om de ulike modulene er tilgjengelig på Sticos' nettsider.

   Kunden har tilgang til de(n) modul(er) som fremgår av avtalen, tilbud og kundens bestilling.

   Ved opprettelse av kundeforholdet skal kunden utpeke en intern administrator for systemet. Den som hos kunden er tillagt rollen som administrator har full tilgang til kundens opplysninger, og er den som tildeler og kontrollerer tilgangen til de øvrige brukere i kundens organisasjon.

   Produktet inkluderer fagsupport. Fagsupport ytes kun til brukere hos kunden som er tildelt rollen som administrator, om ikke annet er avtalt. Fagsupporten dekker generelle spørsmål innenfor de fagområder som er omfattet av produktet, og omfatter ikke råd eller veiledning om tolkning, forståelse eller anvendelse av regelverket i den enkelte kundes konkrete situasjon. Sticos AS forbeholder seg retten til å velge om spørsmål til fagsupport besvares muntlig eller skriftlig.

   Produktet inkluderer nødvendig teknisk kundestøtte i forbindelse med pålogging og bruk av produktet. Teknisk brukerstøtte gis via telefon eller fjernstyring. Med mindre annet er særskilt avtalt med kunden, har alle kundens brukere rett til å melde inn behov om teknisk brukerstøtte.

   Sticos AS vil løpende oppdatere og vedlikeholde regelverk og øvrig innhold i Sticos Personal, og kunden vil gis informasjon om større endringer i produktet. Kunden er selv ansvarlig for oppdatering av sitt eget innhold i produktet.

   Det blir tatt sikkerhetskopi av alle data som kunden oppbevarer hos Sticos AS. Det

oppbevares løpende sikkerhetskopi for de siste 30 dager. Kunden er selv ansvarlig for lagring og sikkerhetskopiering av data som kunden lagrer lokalt hos seg.

En utfyllende beskrivelse av produktet er tilgjengelig på https://sticos.no/produkter/sticos-personal.

## 3. Brukerbegrensninger

Med mindre annet er skriftlig avtalt, plikter den enkelte kunde å oppgi korrekt antall ansatte ved oppstart av avtalen, og skal videre melde fra skriftlig om endringer i antallet ansatte i løpet av avtaleperioden. Tilgang til systemet gis kun for ansatte tilknyttet kundens virksomhet. Hver enkelt bruker identifiseres i systemet gjennom en individuell registrering.

Det er ikke adgang til å opprette tilgang for brukere utenfor kundens egen organisasjon om ikke annet er skriftlig avtalt.

Kunden plikter å sikre at produktet eller deler av dette, ikke skal kopieres eller på annen måte gjøres tilgjengelig for tredjeparter som ikke omfattes av avtalen.

## 4. Tilgjengelighet

Sticos Personal vil normalt være tilgjengelig alle dager i tidsrommet 00.00 til 24.00.

Fagsupport sendes til Sticos AS gjennom egen supportfunksjon i produktet. Sticos tar forbehold om at fagsupport helt eller delvis kan være ubemannet i kortere perioder i forbindelse med ferie, høytider eller i ekstraordinære tilfeller, noe som kan medføre lengre svartid i disse periodene.

Teknisk brukerstøtte og administrative spørsmål kan sendes til Sticos AS hele døgnet pr. epost eller via egen supportfunksjon i produktet. Sticos AS sitt sentralbord er også åpent for mottak av slike supportsaker innenfor normal kontortid. Sentralbordets åpningstider publiseres på https://sticos.no/kontakt.

Dersom det oppstår feil utenfor normal arbeidstid, vil feilretting påbegynnes neste virkedag. Utilgjengelighet som følge av vedlikehold vil så langt det er mulig foretas utenfor normal arbeidstid.

## 5. Tekniske systemkrav

Produktet kan benyttes med operativsystemer og nettlesere som er mest vanlige i markedet til enhver tid. Fullstendig oversikt over systemkrav publiseres på https://support.sticos.no/kunnskapsbase.

Endringer i systemkrav som kan påvirke kundens bruk av systemet varsles med minimum 30 dagers varsel.

## 6. Priser og betalingsbetingelser

Om ikke annet er avtalt har produktet en etableringspris og en abonnementspris for bruk, vedlikehold og support.

I tillegg kommer pris for eventuell bruk av tilleggstjenester som elektronisk signering, samt pris for lagring av kundens data som overstiger 10 GB totalt for alle produkter kunden har fra

Sticos AS. Kunden vil varsles når grensen for avtalt lagringsmengde er nær. Kunden må skriftlig bekrefte avtale om økt lagringsmengde.

Nødvendig teknisk brukerstøtte i forbindelse med pålogging og bruk av produktet inngår i abonnementet. Ved feilsituasjoner meldt til Sticos sin tekniske brukerstøtte som er forårsaket av kundens brukere, kundens infrastruktur eller tredjeparts leverandører som kunden benytter, kan Sticos AS fakturere kunden for den tid som går med til feilsøking og utbedring av feilen.

Gjeldende priser for tilleggstjenester, datalagring og betalbar teknisk brukerstøtte publiseres på https://www.sticos.no/lisensbetingelser/tilleggstjenester.

Alle priser kan justeres ved inngangen til ny avtaleperiode.

Sticos AS fakturerer abonnementsprisen forskuddsvis for kommende avtaleperiode (12 måneder) om ikke annet er avtalt. Sticos AS fakturerer på samme måte - på vegne av tredjepart - eventuelle integrerte løsninger fra tredjepart som kunden har kjøpt gjennom Sticos AS.

Eventuelle endringer i løpet av avtaleperioden som medfører krav om tilleggsbetaling, f.eks. økning i antall ansatte, økt lagringsmengde eller bruk av tilleggstjenester, faktureres fortløpende.

Konsekvensene ved oppsigelse av avtalen i løpet av avtaleperioden er regulert i avtalens pkt. 13

Betalingsbetingelsene er pr. 14 dager fra fakturadato. Ved forsinket betaling beregnes forsinkelsesrente i henhold til Lov om renter ved forsinket betaling.

Bestemmelsene i dette punktet kan fravikes gjennom skriftlig avtale.

## 7. Eiendomsrett

Sticos AS og eventuelle underleverandører har opphavsrett og alle andre immaterielle rettigheter til alle deler av produktet og dets innhold. Dette gjelder ikke kundens egne data.

Kunden og kundens brukere har ikke rett til kopiering, massenedlasting eller automatisk nedlasting av hele eller deler av produktet utover det som er nødvendig for alminnelig bruk, uten etter skriftlig samtykke fra Sticos AS.

## 8. Personvern

Sticos AS lagrer følgende informasjon om sine kunder; informasjon som er avgitt i forbindelse med avtaleinngåelsen, samt senere informasjon om tjenester og produkter som kunden bestiller. Opplysningene benyttes som grunnlag for oppfyllelsen av avtalen, herunder fakturering og regnskapsførsel.

Sticos AS vil oppbevare opplysninger om Kunden også etter utløpet av Avtalen med tanke på senere fornyelse av abonnementsforholdet, og for utsendelse av informasjon om Sticos AS' produkter og tjenester.

Sticos AS vil ved opprettelse av tilganger og ved bruk av produkt og tjenester registrere informasjon om brukeren. Sticos AS kan foreta endringer i behandling av opplysninger og informasjon innenfor rammene av de til enhver tid gjeldende avtaler eller samtykker.

Oppdatert informasjon er på et hvert tidspunkt tilgjengelig på https://www.sticos.no/personvern.

Kunden kan selv be om at Sticos Personal integreres med enkelte tredjepart-systemer som f.eks. timeregistreringssystemer. Nødvendige opplysninger vil i denne sammenheng overføres til denne tredjeparten. Kunden har selv ansvar for å sikre overholdelse av personvernregler og annet relevant regelverk i forbindelse med slik overføring.

Nærmere bestemmelser om databehandling er regulert i egen databehandleravtale som følger som vedlegg 1 til denne avtalen.

## 9. Databehandling

I den utstrekning systemet gjør det mulig for kunden å lagre egne opplysninger hos Sticos AS, vil dette innebære at Sticos AS ved oppbevaring av personopplysninger for kunden opptrer som en databehandler. Kunden er ansvarlig for at behandlingen av opplysningene er i henhold til gjeldende lovgivning.

Sticos AS skal behandle alle data i samsvar med kravene i den til enhver tid gjeldende lovgivning.

Nærmere bestemmelser om databehandling, herunder bruk av underleverandører, er regulert i egen databehandleravtale som følger som vedlegg 1 til denne avtalen.

For å kunne overholde rettighetene og forpliktelsene i kundeavtalen og tilby tilleggsmoduler, utvidelser, produktforbedringer og tilhørende tjenester kan Sticos dele opplysninger om Kunden og Kundens bruk av produktet med andre selskaper. Denne adgangen til deling gjelder kun overfor selskaper i Visma-konsernet, leverandører, partnere og andre tredjeparter som Sticos har et kommersielt samarbeid med knyttet til produktet. Adgangen til deling inkluderer ikke Kundens egne data og personopplysninger ut over det som er avtalt i Vedlegg 1 Databehandleravtale.

## 10. Konfidensialitet, innsyn og revisjon

Innenfor rammene av denne avtalen forplikter Sticos seg til å bevare absolutt taushet overfor uvedkommende om forhold og opplysninger selskapet kommer i befatning med som følge av kundeforholdet. Taushetsplikten gjelder også opplysninger om tredjepart som kommer Sticos til kjennskap som følge av kundeforholdet, som f.eks. klientopplysninger, regnskapsdata og opplysninger om ansatte.

Sticos vil sørge for at alle ansatte utviser aktsomhet ved behandling av sensitive opplysninger og at tekniske systemer er på plass for å sikre at ikke informasjon kommer på avveie.

Taushetsplikten gjelder tilsvarende for Sticos sine eventuelle underleverandører. Taushetsplikten er tidsubegrenset og gjelder også etter at avtaleforholdet er opphørt.

Bestemmelsene i dette punktet er ikke til hinder for påkrevd utlevering av informasjon i henhold til gjeldende lovbestemmelser. Dersom Kundens virksomhet omfattes av Finanstilsynsloven og/eller IKT-forskriften gjelder dette også Finanstilsynets rett til tilgang til nødvendige opplysninger som ledd i tilsynet med Kunden og tilsyn med utkontraktert virksomhet (Sticos AS og deres underleverandører) uten begrensninger, jf. Finanstilsynsloven § 4c og IKT-forskriften § 12. Kunden har også selv krav på nødvendig informasjon og

rapporter fra Sticos AS og deres underleverandører for at foretaket skal kunne følge opp sin utkontrakterte virksomhet og oppfylle foretakets egne rapporteringsplikter i den forbindelse.

For kunder som omfattes av IKT-forskriften har både Kunden og Finanstilsynet rett til å utføre nødvendig revisjon av utkontraktert virksomhet hos Sticos AS og deres underleverandører..

I en beredskapssituasjon skal Sticos AS samarbeide med norske myndigheter i samsvar med lovpålagte krav i relevant sektorregelverk som Kunden omfattes av.

## 11. Ansvar

Til tross for omfattende kvalitetssikring av innhold og funksjoner i produktet er det umulig for Sticos å sikre seg mot alle mulige feil i innhold og funksjoner utviklet av Sticos eller levert av tredjeparter. Kunden plikter selv å kvalitetssikre informasjon som kan forårsake skade ved feil eller ufullstendigheter.

Kundens bruk av produktet erstatter ikke konkret juridisk rådgivning. Kunden er ansvarlig for egen tolkning og bruk av produktets innhold og funksjoner. Kunden må vurdere i den enkelte sak om og i hvilken utstrekning det aktuelle innholdet er oppdatert og passer formålet, herunder om innholdet bør tilpasses eller modifiseres for å ivareta kundens behov.

Sticos fraskriver seg ethvert ansvar som følge av Kundens bruk av produktet, herunder opplysninger gitt i forbindelse med fagsupport og brukerstøtte, med unntak for tilfeller som følger av grov uaktsomhet eller forsett. Sticos sitt samlede erstatningsansvar i avtaleperioden er i alle tilfeller begrenset oppad til et beløp som tilsvarer vederlaget som er fakturert for Sticos Personal de siste 12 månedene før mangelen oppstod. Indirekte tap dekkes ikke. Indirekte tap omfatter, men er ikke begrenset til, tapt fortjeneste av enhver art, tapte besparelser, tap av data, tilfeldige tap, eller krav fra tredjeparter.

Om produktet i vesentlig grad skulle være utilgjengelig for kunden hverdager mellom kl. 07:00 og kl. 19:00 grunnet forhold som Sticos AS er ansvarlig for, kan kunden kreve forholdsmessig prisavslag. Som vesentlig anses når produktet i sin helhet er utilgjengelig mer enn 0,5 % av garantert oppetid pr. kalendermåned.

For å sikre kvaliteten på systemet bør eventuelle feil som kunden blir oppmerksom på meldes til Sticos AS så snart som mulig.

## 12. Mislighold

Ved betalingsmislighold har Sticos AS rett til å sperre tilgangen til Sticos Personal og fagsupporten uten nærmere forvarsel, frem til betaling har funnet sted.

Sticos AS har rett til umiddelbart å si opp avtalen eller begrense enkeltbrukeres tilgang til hele eller deler av produktet (herunder fagsupport) dersom kunden eller kundens brukere vesentlig misligholder abonnementsavtalen. Opphør av avtalen medfører at tilgangen til Sticos Personal og fagsupport blir sperret.

Mislighold fra kundens side reduserer ikke kundens forpliktelse til å betale abonnementspris for avtaleperioden.

Ved vesentlig mislighold av avtalen fra Sticos AS sin side, og som Sticos AS ikke har klart å rette innen rimelig tid etter skriftlig varsel fra kunden, kan kunden heve avtalen med øyeblikkelig virkning. Vesentlig mislighold av avtalen fra Sticos AS sin side medfører forholdsmessig refusjon av betalt abonnementspris for avtaleperioden.

## 13. Varighet og oppsigelse

Avtalen trer i kraft fra det tidspunkt Kunden bestiller abonnement på Sticos Personal.

Ved utløpet av avtaleperioden etter pkt. 1 fornyes avtalen automatisk for en ny avtaleperiode på 12 måneder med mindre avtalen sies opp skriftlig av en av partene. Oppsigelsen får virkning fra utløpet av inneværende avtaleperiode.

Konsekvensen av en oppsigelse er at tilgangen til produktet stenges og at Sticos sletter kundens data 6 måneder etter at avtalen har opphørt. Kunden er selv ansvarlig for å innhente rapporter, egne dokumenter og sine øvrige data fra produktet innen utløpet av avtaleperioden, og sørge for egen oppbevaring av disse i tiden etter.

Bestemmelsene i dette punktet kan fravikes gjennom skriftlig avtale.

## 14. Tvister

Avtalen er underlagt norsk lov.

Tvister mellom partene skal søkes løst ved forhandlinger. Dersom det ikke lykkes å oppnå en enighet i løpet av en periode på 60 dager, har hver av partene rett til å bringe tvisten inn for rettslig behandling.

For tvister som oppstår i forbindelse med denne avtalen benyttes den rettskrets hvor Sticos AS har sitt hovedkontor som verneting.

## 15. Vedlegg

Vedlegg 1: Databehandleravtale

Vedlegg 2: Data processing agreement

Vedlegg 1 til lisensavtale for Sticos Personal

**Databehandleravtale**

mellom Kunden og

| | |
|---|---|
| **Databehandler:** | Sticos AS |
| Organisasjonsnummer: | 934 228 391 |
| Etablert i: | Norge |
| Databehandlerens kontaktinformasjon for generelle henvendelser: | personvern@sticos.no |
| Databehandlerens kontaktinformasjon for henvendelser om uautorisert behandling av personopplysninger: | personvern@sticos.no<br>Sticos Kundesenter, Tlf.: 73 56 00 00 |

heretter betegnet som henholdsvis Behandlingsansvarlig, Databehandler eller Part, i fellesskap som Partene.

**Innledning**

Partene bekrefter herved at de har nødvendige fullmakter til å inngå denne databehandleravtalen (Databehandleravtalen). Databehandleravtalen vil utgjøre en del av og regulere all behandling av personopplysninger i tilknytning til avtale om levering av tjenester (Tjenesteavtale) mellom partene:

- Lisensavtale Sticos Personal

**Definisjoner**

Definisjonene av personopplysning, særlige kategorier av personopplysning, behandling av personopplysning, den registrerte, behandlingsansvarlig og databehandler skal forstås slik de brukes og tolkes i henhold til gjeldende personvernlovgivning, inkludert lov om behandling av personopplysninger av 15. juni 2018 nr. 38 og personvernforordningen Europaparlaments- og rådsforordning (EU) 2016/679 (GDPR) av 27. april 2016.

**Formål**

Databehandleravtalen regulerer Databehandlerens behandling av personopplysninger på vegne av den Behandlingsansvarlige, og beskriver hvordan Databehandleren gjennom tekniske og organisatoriske virkemidler skal bidra til å sikre den registrertes rettigheter på vegne av den Behandlingsansvarlige.

Formålet med Databehandlerens behandling av personopplysninger er å oppfylle Tjenesteavtalen og Databehandleravtalen.

Ved eventuell motstrid mellom bestemmelser om behandling av personopplysninger har Databehandleravtalen forrang over Tjenesteavtale eller tidligere avtaler inngått mellom Partene.

**Databehandlerens plikter**

Databehandler skal bare behandle personopplysninger på vegne av og i henhold til instruksjoner fra Behandlingsansvarlig. Ved å inngå denne Databehandleravtalen instruerer Behandlingsansvarlig Databehandler om å behandle personopplysninger på følgende måte: i) bare i henhold til gjeldende lovgivning, ii) for å oppfylle alle plikter i henhold til Tjenesteavtale, iii) som instruert via Behandlingsansvarlig sin bruk av Databehandlers ordinære tjenester og iv) som spesifisert i denne Databehandleravtalen.

Databehandleren har ved avtaleinngåelsen ingen grunn til å anta at det foreligger regulatoriske hindringer mot å følge instruksjonene fra Behandlingsansvarlige. Dersom Databehandleren ved et senere tidspunkt blir klar over at Behandlingsansvarliges instruksjoner eller behandling av personopplysninger strider mot gjeldende personvernlovgivning, skal Databehandleren melde dette til Behandlingsansvarlige.

Typen personopplysninger og kategorier av registrerte som er gjenstand for behandling under denne Databehandleravtalen er angitt i vedlegg A.

Databehandleren skal sikre konfidensialitet, integritet og tilgjengelighet til personopplysningene i henhold til de regulatoriske krav som gjelder for Databehandleren. Dette inkluderer å implementere systematiske, organisatoriske og tekniske virkemidler for å sikre et tilstrekkelig nivå for sikkerhet. Ved avgjørelsen av hva som er et tilstrekkelig nivå skal hensyn til den teknologiske utviklingen og kostnaden ved implementering av tiltak veies mot risikoen ved behandlingen og typen personopplysninger som behandles.

Databehandleren skal ved tekniske og organisatoriske virkemidler bistå Behandlingsansvarlig med å ivareta Behandlingsansvarliges plikter under GDPR artikkel 32 til 36, samt bistå i arbeidet med å behandle forespørsler fra registrerte i henhold til GDPR kapittel III. Pliktens omfang avgrenses av formen for behandling av personopplysninger og hvilken informasjon som er tilgjengelig for Databehandleren.

Behandlingsansvarlige kan kreve informasjon om de sikkerhetstiltak, dokumentasjon og annen informasjon om hvordan Databehandleren behandler personopplysninger. Dersom Behandlingsansvarlige ber om mer informasjon eller assistanse enn det som Databehandleren tilgjengeliggjør for å oppfylle kravene til rollen som Databehandler i henhold til gjeldende personvernlovgivning, kan Databehandleren kreve betaling for slike eventuelle tilleggstjenester.

Databehandleren og dennes ansatte skal sørge for konfidensialitet ved behandling av personopplysninger som behandles i henhold til denne databehandleravtalen. Denne plikten gjelder også etter at avtalen opphører.

Databehandleren vil gjennom å varsle Behandlingsansvarlig uten ugrunnet opphold om brudd på personopplysningssikkerheten, muliggjøre etterlevelse av gjeldende personvernlovgivning vedrørende varsling av tilsynsmyndigheter og registrerte.

Videre vil Databehandleren, i den utstrekning det er praktisk mulig og lovlig, varsle Behandlingsansvarlig om;

i) innsynsbegjæringer fra registrerte,

ii) innsynsbegjæringer fra offentlige myndigheter

Databehandleren vil kun besvare forespørsler fra registrerte i den grad Behandlingsansvarlig har gitt tillatelse til det. Databehandleren vil kun varsle Behandlingsansvarlig om innsynsbegjæringer fra offentlige myndigheter i den grad slikt varsel er lovlig, samt kun utlevere informasjon til offentlige myndigheter dersom rettslig pålegg foreligger.

Databehandleren har ikke eierskap til eller kontroll med hvorvidt og hvordan Behandlingsansvarlig velger å benytte seg av eventuelle tredjeparts integrasjoner via Databehandlers API, via direkte databasekobling eller lignende. Ansvaret for slike integrasjoner med tredjepart påhviler utelukkende Behandlingsansvarlig.

**Behandlingsansvarliges plikter**

Ved å signere Databehandleravtalen bekrefter Behandlingsansvarlig:

- Behandlingsansvarlig har rett til å behandle personopplysninger og til å gi Databehandleren og dennes underleverandører adgang til å behandle personopplysninger.
- Behandlingsansvarlig er ansvarlig for at personopplysningene som overlates til Databehandleren er lovlig innsamlet, korrekte og tilstrekkelige.
- Behandlingsansvarlig er ansvarlig for å gi relevant informasjon til registrerte eller myndigheter vedrørende behandlingen av personopplysninger.
- Særlige kategorier av personopplysninger vil bare bli behandlet som en del av Tjenesteavtalen der dette er uttrykkelig avtalt i Vedlegg A til Databehandleravtalen.

**Bruk av underleverandører og overføring av personopplysninger**

Som en del av leveransen under Tjenesteavtale vil Databehandleren bruke underleverandører og Behandlingsansvarlig gir sitt generelle samtykke til dette. Slike underleverandører kan være andre selskaper i konsernet eller eksterne tredjeparter. Databehandleren har plikt til å påse at underleverandører påtar seg tilsvarende forpliktelser som de som følger av denne Databehandleravtalen.

Oversikt over underleverandører med tilgang til personopplysninger fremgår på adressen https://www.sticos.no/personvern/trust. I tillegg kan Behandlingsansvarlig ta kontakt med Databehandler for mer detaljert informasjon om underleverandører.

Dersom underleverandøren er lokalisert utenfor EU/EØS gir Behandlingsansvarlig fullmakt til Databehandleren til å sikre lovlig overføringsgrunnlag for overføringen av personopplysninger ut av EU/EØS på vegne av Behandlingsansvarlig, herunder ved å gjøre bruk av EU standardavtaler.

Behandlingsansvarlig vil bli varslet før Databehandleren endrer underleverandør som behandler personopplysninger. Dersom Behandlingsansvarlig kommer med innsigelser til underleverandører i denne forbindelse skal partene tilgjengeliggjøre og gjennomgå informasjon og dokumentasjon om underleverandøren som påviser dens etterlevelse av personvernlovgivningen. Dersom behandlingsansvarlig motsetter seg ny bruk eller bytte av underleverandør har partene rett til å si opp avtalen med virkning fra dato for oppstart av behandling hos underleverandøren.

**Sikkerhet**

Databehandler skal sørge for et høyt sikkerhetsnivå i sine produkter og tjenester. Dette skal skje ved organisatoriske, tekniske og fysiske sikkerhetstiltak, i henhold til kravene til informasjonssikkerhet som fremgår av GDPR artikkel 32.

Visma-konsernets rammeverk for personvern skal sikre personopplysningenes konfidensialitet, integritet, robushet og tilgjengelighet. Følgende tiltak er særlig viktig i denne forbindelse:

- Klassifisering av personopplysninger for å vurdere sikkerhetstiltakene på bakgrunn av risikovurderinger.
- Vurdere bruk av kryptering og pseudonymisering for å avhjelpe risiko.
- Begrense tilgang til personopplysninger til personell som trenger tilgang for å oppfylle plikter i henhold

til denne Databehandleravtalen eller Tjenesteavtale.

- Systemer som avdekker, retter, forhindrer og rapporterer avvik.
- Benytte sikkerhetsrevisjoner til å analysere hvorvidt de til enhver tids gjeldende tekniske og organisatoriske tiltak for å beskytte personopplysninger er tilstrekkelig, sett i lys av gjeldende lovgivning.

**Rett til tilsyn**

Behandlingsansvarlig kan revidere Databehandler sin etterlevelse av denne Databehandleravtalen inntil en gang i året. Hvis lovgivning som Behandlingsansvarlig er underlagt krever det, kan Behandlingsansvarlig kreve flere revisjoner.

For å be om revisjon må Behandlingsansvarlig sende en detaljert tilsynsplan minimum 4 uker i forkant av ønsket tilsynsdato, med oversikt over forslagets omfang, varighet og oppstart. Hvis tredjeparter skal gjennomføre tilsynet, skal dette som hovedregel avtales mellom Partene. Hvis behandling av personopplysninger skjer i et "multitenant" miljø eller lignende, aksepterer Behandlingsansvarlig likevel at tilsynet gjennomføres av en tredjepart utpekt av Databehandler.

Hvis tilsynets omfang er behandlet i ISAE, ISO eller lignende rapport av kvalifisert tredjepart i løpet av de siste 12 månedene, og Databehandler bekrefter at det ikke finnes kjente endringer fra dette, skal Behandlingsansvarlig akseptere disse rapportene i stedet for å forespørre nytt tilsyn.

I alle tilfeller skal tilsyn utføres i samråd med virksomhetens ordinære åpningstider, i henhold til virksomhetens retningslinjer og ikke forstyrre den ordinære virksomheten. Behandlingsansvarlig er ansvarlig for kostnader forårsaket av sitt tilsyn. Dersom Behandlingsansvarlige ber om mer assistanse enn den som tilbys av Databehandleren for å oppfylle gjeldende personvernlovgivning, kan Databehandleren kreve betaling for denne tilleggstjenesten.

**Varighet**

Databehandleravtalen gjelder så lenge Databehandler behandler personopplysninger på vegne av Behandlingsansvarlig i henhold til Tjenesteavtale.

Databehandleravtalen opphører i forbindelse med avslutning av Tjenesteavtale. Ved opphør av Databehandleravtalen, skal Databehandler slette eller returnere personopplysninger som er behandlet på vegne av Behandlingsansvarlig i tråd med Tjenesteavtale. Med mindre annet er avtalt mellom Partene, skal arbeidet forbundet med dette kompenseres basert på; i) kompleksiteten ved forespørselen og ii) betaling for medgått tid. Slik forespørsel må rettes Sticos innen 6 måneder etter avtalens opphør.

Databehandler kan beholde personopplysninger etter opphøret av Databehandleravtalen i henhold til gjeldende lovgivning, underlagt de samme typer tekniske og organisatoriske tiltak som skissert i denne Databehandleravtalen.

**Endringer og ugyldighet**

Endringer i Databehandleravtalen skal inkluderes i ny avtale eller i et eget endringsvedlegg og aksepteres av begge Parter for å være gyldig..

Hvis bestemmelser i Databehandleravtalen kjennes ugyldig, skal ikke dette påvirke de øvrige bestemmelsene i Databehandleravtalen. Partene skal erstatte den ugyldige bestemmelsen med en gyldig bestemmelse som reflekterer intensjonen til Partene bak bestemmelsen.

**Mislighold**

Begge parter har et individuelt ansvar etter gjeldende personvernlovgivning i forhold til de personopplysningene de behandler og skal holdes selvstendig ansvarlig for å betale alle bøter og erstatning direkte til registrerte som ilegges den respektive part av myndigheter eller domstoler i henhold til personvernlovgivningen.  Ansvaret mellom partene reguleres av Tjenesteavtalen.

**Gjeldende rett og verneting**

Databehandleravtalen er underlagt norsk rett ved norske domstoler med Trondheim tingrett som avtalt verneting.

**Vedlegg**

Vedlegg A - Kategorier av registrerte og personopplysninger

**Vedlegg A - Kategorier av registrerte og personopplysninger**

1. *Kategorier av registrerte og personopplysninger*

    a. Kategorier av registrerte
        i. kundens sluttbruker
        ii. ansatt hos kunde
        iii. kontaktpersoner hos kunde
    b. Kategorier av personopplysninger
        i. kontaktinformasjon som navn, telefon, adresse, e-postadresse mv.
        ii. jobbrelatert informasjon som tittel, arbeidsgiver, mv.
        iii. økonomisk informasjon som kortnummer, faktura, konto etc.
        iv. bruksdata og innloggingsinformasjon, som brukerID, innloggingstidspunkt, søkehistorikk, mv.
        v. brukerens egen input som følge av bruk av tjenesten, som innhold i avviksrapportering, skjema, egne innlagte tekster, oppgavelister, opplastede dokumenter, mv.
        vi. opplysninger avgitt ved support, som beskrivelse av sak og eventuelle vedlegg, mv.
        vii. feilsøkingslogger
        viii. HR-opplysninger, dersom disse funksjonene er aktivert av kunden, som ferie, permisjoner, sykefravær, kompetanse, mv.

Attachment 1 to Licence agreement Sticos Personal (translated)

## Data Processing Agreement

between the Customer and

| | |
|---|---|
| **Data Processor:** | Sticos AS |
| Organisation number: | 934 228 391 |
| Country of establishment: | Norway |
| Data Processor's contact for general requests: | personvern@sticos.no |
| Data Processor's contact for notification of unauthorised data processing: | personvern@sticos.no<br>Sticos Customer Service, Tlf.: 73 56 00 00 |

Henceforth respectively referred to as "Controller", "Processor", or "Party" and collectively as the "Parties".

### Introduction

Both Parties confirm that the undersigned have the power of attorney to enter into this data processing agreement ("Agreement"). This Agreement will form part of and regulate the processing of personal data tied to the following service agreements ("Service Agreements") between the Parties:

- Lisensavtale Sticos Personal

### Definitions

The definition of Personal Data, Special Categories of Personal Data (Sensitive Personal Data), Processing of Personal Data, Data Subject, Controller and Processor is equivalent to how the terms are used and interpreted in applicable privacy legislation, including the General Data Protection Regulation (GDPR) applicable for this Agreement and Europe from 25 May 2018.

### Scope

The Agreement regulates the Processor's Processing of Personal Data on behalf of the Controller, and outlines how the Processor shall contribute to ensure privacy on behalf of the Controller and its registered Data Subjects, through technical and organisational measures according to applicable privacy legislation, including the GDPR.

The purpose behind the Processor's Processing of Personal Data on behalf of the Controller is to fulfill the Service Agreements and this Agreement.

This Agreement takes precedence over any conflicting provisions regarding the Processing of Personal Data in the Service Agreements or in other former agreements made between the Parties. The original Norwegian text takes precedence over this translation.

**The Processor's obligations**

The Processor shall only Process Personal Data on behalf of and in accordance with the Controller's instructions. By entering into this Agreement, the Controller instructs the Processor to process Personal Data in the following manner; i) only in accordance with applicable law, ii) to fulfill all obligations according to the Service Agreement, iii) as further specified via the Controller's ordinary use of the Processor's services and iv) as specified in this Agreement.

The Processor has no reason to believe that legislation applicable to it prevents the Processor from fulfilling the instructions mentioned above. The Processor shall, upon becoming aware of it, notify the Controller of instructions or other Processing activities by the Controller which in the opinion of the Processor, infringes applicable privacy legislation.

The categories of Data Subject's and Personal Data subject to Processing according to this Agreement are outlined in Appendix A.

The Processor shall ensure the confidentiality, integrity and availability of Personal Data according to privacy legislation applicable to The Processor. The Processor shall implement systematic, organisational and technical measures to ensure an appropriate level of security, taking into account the state of the art and cost of implementation in relation to the risk represented by the Processing, and the nature of the Personal Data to be protected.

The Processor shall assist the Controller by appropriate technical and organisational measures, insofar as possible and taking into account the nature of the Processing and the information available to the Processor, in fulfilling the Controller's obligations under applicable privacy legislation with regards to request from Data Subjects, and general privacy compliance under the GDPR article 32 to 36.

If the Controller requires information or assistance regarding security measures, documentation or other forms of information regarding how the Processor processes Personal Data, and such requests exceed the standard information provided by the Processor to comply with applicable privacy legislation as Processor, the Processor may charge the Controller for such request for additional services.

The Processor and its staff shall ensure confidentiality concerning the Personal Data subject to Processing in accordance with the Agreement. This provision also applies after the termination of the Agreement.

The Processor will, by notifying the Controller without undue delay, enable the Controller to comply with the legal requirements regarding notification to data authorities or Data Subjects about incidents.

Further, the Processor will to the extent it is appropriate and lawful notify the Controller of;

i) requests for the disclosure of Personal Data received from a Data Subject,

ii) requests for the disclosure of Personal Data by governmental authorities, such as the police

The Processor will not respond directly to requests from Data Subjects unless authorised by the Controller to do so. The Processor will not disclose information tied to this Agreement to governmental authorities such as the police, hereunder Personal Data, except as obligated by law, such as through a court order or similar warrant.

The Processor does not control if and how the Controller uses third party integrations through the Processor's API or similar, and thus the Processor has no ownership to risk in this regard. The Controller is solely responsible for third party integrations.

**The Controller's obligations**

The Controller confirms by the signing of this Agreement that:

- The Controller has legal authority to process and disclose to the Processor (including any subcontractors used by the Processor) the Personal Data in question.
- The Controller has the responsibility for the accuracy, integrity, content, reliability and lawfulness of the Personal Data disclosed to the Processor.
- The Controller has fulfilled its duties to provide relevant information to Data Subjects and authorities regarding processing of Personal Data according to mandatory data protection legislation.
- The Controller shall, when using the services provided by the Processor under the Services Agreement, not communicate any Sensitive Personal Data to the Processor, unless this is explicitly agreed in Appendix A to this Agreement.

**Use of subcontractors and transfer of data**

As part of the delivery of services to the Controller according to the Service Agreements and this Agreement, the Processor will make use of subcontractors and the Controller gives its general consent to usage of subcontractors. Such subcontractors can be other companies within the Visma group or external third party subcontractors. The Processor shall ensure that subcontractors agrees to undertake responsibilities corresponding to the obligations set out in this Agreement.

An overview of the current subcontractors with access to Personal Data can be found at https://www.sticos.no/personvern/trust. The Controller may request more detailed information about subcontractors.

If the subcontractors are located outside the EU, the Controller gives the Processor authorisation to ensure proper legal grounds for the transfer of Personal Data out of the EU on behalf of the Controller, hereunder by entering into EU Model Clauses.

The Controller shall be notified in advance of any changes of subcontractors that Process Personal Data. If the Controller objects to a new subcontractor, the Processor and Controller shall review the documentation of the subcontractors compliance efforts in order to ensure fulfillment of applicable privacy legislation.

**Security**

The Processor is committed to provide a high level of security in its products and services. The Processor provides its security level through organisational, technical and physical security measures, according to the requirements on information security measures outlined in the GDPR article 32.

The Visma-group's framework for privacy shall ensure the confidentiality, integrity, robustness and accessibility of personal data. The following measures are of particular importance:

- Classification of personal data to assess security measures based on risk assessment.
- Consider encryption and pseudonymization to mitigate risk.
- Restrict access to personal data only to personnel who need such access to fulfill obligations under this Data Protection Agreement or Service Agreement.
- Implementation of systems that detect, correct, prevent and report deviations.
- Use security audits to analyse whether current technical and organisational measures to protect personal data are sufficient, in light of current legislation.

**Audit rights**

The Controller may audit the Processor's compliance with this Agreement up to once a year. If required by legislation applicable to the Controller, the Controller may request audits more frequently.

To request an audit, the Controller must submit a detailed audit plan at least four weeks in advance of the proposed audit date to the Processor, describing the proposed scope, duration, and start date of the audit. If any third party is to conduct the audit, it must as a main rule be mutually agreed between the Parties. However, if the processing environment is a multitenant environment or similar, the Controller gives the Processor authority to decide, due to security reasons, that audits shall be performed by a neutral third party auditor of the Processor's choosing.

If the requested audit scope is addressed in an ISAE, ISO or similar assurance report performed by a qualified third party auditor within the prior twelve months, and the Processor confirms that there are no known material changes in the measures audited, the Controller agrees to accept those findings instead of requesting a new audit of the measures covered by the report.

In any case, audits must be conducted during regular business hours at the applicable facility, subject to the Processors policies, and may not unreasonably interfere with the Processors business activities.

The Controller shall be responsible for any costs arising from the Controller's requested audits. Requests for assistance beyond what is required to comply with current privacy legislation from the Processor may be subject to fees.

**Term and termination**

This Agreement is valid for as long as the Processor processes Personal Data on behalf of the Controller according to the Service Agreements.

This Agreement is automatically terminated upon termination of the Service Agreement. Upon termination of this Agreement, the Processor will delete or return Personal Data processed on behalf of the Controller, according to the applicable clauses in the Service Agreement. Unless otherwise agreed in writing, the cost of such actions shall be based on; i) hourly rates for the time spent by the Processor and ii) the complexity of the requested process.

The Processor may retain Personal Data after termination of the Agreement, to the extent it is required by law, subject to the same type of technical and organisational security measures as outlined in this Agreement.

**Changes and amendments**

Changes to the Data Processor Agreement shall be included in a new agreement or in an Appendix to this agreement and accepted by both Parties in order to be valid.

If any provisions in this Agreement become void, this shall not affect the remaining provisions. The Parties shall replace the void provision with a lawful provision that reflects the purpose of the void provision.

**Liability**

The Parties agree and acknowledge that each Party shall be liable for and held accountable to pay administrative fines and damages directly to data subjects which the Party has been imposed to pay by the data protection authorities or authorised courts according to applicable privacy legislation. Liability matters between the Parties shall be governed by the liability clauses in the Service Agreement between the Parties.

**Governing law and legal venue**

This Agreement is subject to the governing law and legal venue as set out in the Service Agreement between the parties.

**Attachments**

Appendix A - Categories of Personal Data and Data Subjects

**Appendix A - Categories of Personal Data and Data Subjects**

1. *Categories of Data Subject's and Personal Data subject to Processing according to this Agreement*

    *a.* Categories of Data Subjects
        i. customer end users
        ii. customer employees
        iii. customer contact persons
    b. Categories of Personal Data
        i. contact information such as name, phone, address,email etc.
        ii. job information such as position, company etc
        iii. economical information such as credit card, invoice, account, etc.
        iv. usage statistics and login information, such as userID, login time, search history, etc.
        v. the user's own input as a result of using the service, such as content in non-conformance reports, forms, user text and edits, uploaded documents, etc.
        vi. information provided to support, such as description of the issue, attachments, etc.
        vii. HR data, should these functions be activated, such as holidays, leave, sick leave, competence, etc.