

Databehandleravtale

mellom

Rennebu kommune
«Behandlingsansvarlig»

og

Sem & Stenersen Prokom AS
Org.nr. 953 675 358
«Databehandler»

1. Avtalens hensikt og definisjoner

I forbindelse med levering av ytelser etter denne avtale, vil Databehandler behandle personopplysninger på vegne av Behandlingsansvarlig.

Databehandleravtalen skal sikre at personopplysninger ikke brukes urettmessig eller kommer uberettigede i hende, sikre personopplysningens integritet, konfidensialitet og tilgjengelighet og at de for øvrig behandles i samsvar med krav i lover og regler, herunder den til enhver tid gjeldende personopplysningslov.

EUs nye personvernforordning EU 2016/679 – GDPR («Personvernforordningen») er implementert i ny personopplysningslov av 15.juni 2018 nr 38 som trådte i kraft 20.juli 2018. Denne avtalen er ment å være i samsvar med denne personopplysningsloven med tilhørende EU personvernforordning (GDPR), men Partene er enige om at Avtalen skal endres dersom det er nødvendig for å bringe den i samsvar med den til enhver tid gjeldende personopplysningslov dersom det viser seg at avtalen ikke ivaretar forpliktelsene etter gjeldende regelverk.

Avtalen regulerer all bruk av Sem & Stenersen Prokom AS, som databehandler (heretter «Databehandler»), personopplysninger på vegne av [KUNDEN] som behandlingsansvarlig (heretter «Behandlingsansvarlig»), herunder, men ikke begrenset til, Innsamling, registrering, sammenstilling, lagring, utlevering eller kombinasjoner av disse, i forbindelse med leveranse og drift av ~~Chatbot «Kommune-Kari»~~ («Tjenesten»).

Backup

Definisjoner:

- «Behandlingsansvarlig» er fysisk eller juridisk person, en offentlig myndighet, en institusjon eller ethvert annet organ som alene eller sammen med andre bestemmer formålet med behandlingen av personopplysninger og hvilke midler som skal benyttes
- «Databehandler» er den som behandler personopplysninger på vegne av behandlingsansvarlige – i dette tilfellet Sem & Stenersen Prokom AS.
- «Personopplysninger» enhver opplysning om en identifisert eller identifiserbar fysisk person («den registrerte»); en identifiserbar fysisk person er en person som direkte eller indirekte kan identifiseres, særlig ved hjelp av en identifikator, f.eks. et navn, et identifikasjonsnummer, lokaliseringsopplysninger, en online-indikator eller ett eller flere elementer som er spesifikke for nevnte fysiske persons fysiske, fysiologiske, genetiske, psykiske, økonomiske, kulturelle eller sosiale enhet
- «Sensitive personopplysninger» er opplysninger om rasemessig eller etnisk opprinnelse, politisk oppfatning, religion, overbevisning eller fagforeningsmedlemskap, samt behandling av generiske opplysninger og biometriske opplysninger med det formål å entydlig identifisere en fysisk person, helseopplysninger eller opplysninger om en fysisk persons seksuelle forhold eller seksuelle orientering.
- «Behandling» er enhver operasjon eller rekke av operasjoner som gjøres med personopplysninger, enten automatiserte eller ikke, f.eks. Innsamling, registrering, organisering, strukturering, lagring, tilpasning eller endring, gjenfinning, konsultering, bruk, utlevering ved overføring, spredning eller alle andre former for tilgjengliggjøring, sammenstilling eller samkjøring, begrensnig, sletting eller tilintetgjøring.

2. Databehandleravtalens formål og omfang

Databehandler kan ikke behandle personopplysninger på annen måte enn det som er nødvendig for å levere de avtalte ytelser til Behandlingsansvarlig, slik de er nærmere beskrevet i denne avtalen. Behandlingsansvarlig forplikter seg til ikke å behandle personopplysningene til andre formål.

Formålet med lagringen og behandlingen av personopplysningene i SYSTEMET, og hvilke personopplysninger som vil bli lagret og behandlet i SYSTEMET fremgår av **vedlegg 1** til denne avtale.

I tillegg har Databehandler som ledd i oppfyllelse og oppfølging av leveransene i nærværende Avtale, lagret følgende opplysninger om relevante kontaktpersoner hos Behandlingsansvarlige i sitt CRM-verktøy: navn, stilling, telefonnummer og e-postadresse.

3. Databehandlers plikter

Databehandleren skal følge de til enhver tid gjeldende Instruks for behandling av personopplysninger som Behandlingsansvarlig har bestemt skal gjelde gjennom denne Databehandleravtale.

Databehandleren kan kun behandle personopplysninger i samsvar med denne avtalen eller etter annen dokumentert Instruks fra Behandlingsansvarlig. Dersom en Instruks er i strid med gjeldende personvernregelverk, skal Databehandleren straks informere Behandlingsansvarlig om dette. Databehandleren kan ikke overføre personopplysninger til land utenfor EU/EØS uten skriftlig instruks fra Behandlingsansvarlig. Med overføring menes også oppbevaring av opplysninger eller back-up på servere, dersom disse befinner seg utenfor EU/EØS.

Databehandler skal bistå Behandlingsansvarlig med følgende:

- Feilretting, vedlikehold, og oppgradering.
- Filoppretting og flytting av data
- Systemsikkerhet
- Brukerstøtte

Ved gjennomføring av de ulike oppgavene Databehandler skal bistå med kan Databehandler måtte foreta operasjoner som innebærer innsyn i de personopplysningene Behandlingsansvarlig har i SYSTEMET. Slikt innsyn er begrenset til det som er nødvendig for å utføre de oppgaver som Databehandler skal utføre. Databehandler skal varsle Behandlingsansvarlig før slike oppgaver som innebærer innsyn i personopplysningene med mindre hensynet til å ivareta Behandlingsansvarliges interesser tilsier noe annet.

Behandlingsansvarlig har, med mindre annet er avtale eller følger av lov, rett til tilgang til og innsyn i personopplysningene som behandles og systemene som benyttes til dette formål. Databehandler plikter å gi nødvendig bistand til dette.

Databehandleren plikter å ha dokumentert systemer og prosedyrer som er relevante i forbindelse med Avtalen. Med dokumentasjon menes prosedyrer for autorisasjon/bruk og for ulike tekniske og organisatoriske sikkerhetstiltak. Dokumentasjonen skal være tilgjengelig for Behandlingsansvarlig, kommunen, Datatilsynet og eventuelt andre institusjoner. Innsyn i dokumentasjonen skal reguleres strengt og kun gis til et begrenset antall autoriserte personer slik at sikkerhetsnivået ivaretas.

Databehandler har taushetsplikt om dokumentasjon og personopplysninger som Databehandler får tilgang til som følge av denne Avtalen. Denne bestemmelsen gjelder også etter Avtalens opphør. Databehandleren er også ansvarlig for at alle personer hos Databehandleren og eventuelle underleverandører som er autorisert til å behandle personopplysningene, har forpliktet seg til å behandle opplysningene fortrolig eller at de er underlagt tilstrekkelig lovfestet taushetsplikt.

Databehandler plikter ved hjelp av egnede tekniske og organisatoriske tiltak, å bistå Behandlingsansvarlig med å oppfylle sine plikter ovenfor den registrerte etter GDPR kapittel 3. Databehandler skal bistå Behandlingsansvarlig med å sikre overholdelse av kravene til personopplysningssikkerhet, avvikshåndtering, konsekvensanalyse og forhåndsdrøftinger, samt for øvrig ved oppfyllelsen av forpliktelser etter Databehandleravtalen. Databehandleren skal uten ugrunnet opphold bistå Behandlingsansvarlig med å svare på anmodninger fra de Registrerte, slik at de Registrerte kan utøve sine rettigheter etter gjeldende personvernregelverk og Behandlingsansvarlig kan svare på de Registrertes anmodninger Innen gjeldende regelverk. Dersom Databehandler mottar henvendelser fra den registrerte og/eller andre parter relatert til rettigheter etter Databehandleravtalen skal Databehandler uten ugrunnet opphold videresende henvendelsen til Behandlingsansvarlig.

Databehandleren skal bistå Behandlingsansvarlig med å sikre overholdelse av den Behandlingsansvarliges forpliktelser etter gjeldende personvernregelverk, herunder ivareta krav til sikkerhet ved behandlingen i samsvar med punkt 5 nedenfor, bistå med melding til tilsynsmyndigheter og de Registrerte om eventuelle brudd på personvernsikkerheten, bistå med vurdering av personvernkonsekvenser og delta i forhåndsdrøftinger med Datatilsynet før behandling med antatt høy risiko for personvernet.

Databehandleren plikter på anmodning å samarbeide med tilsynsmyndighetene i samsvar med gjeldende personvernregelverk.

4. Bruk av underleverandør

Databehandler kan, innenfor Databehandleravtalens rammer, benytte underleverandører, forutsatt at skriftlig samtykke gis fra Behandlingsansvarlig. Dette forutsetter skriftlig avtale mellom Databehandler og underleverandør, samt tilfredsstillende dokumentasjon for at det blir gjennomført tekniske og organisatoriske tiltak som sikrer at kravene i Databehandleravtalen er oppfylt.

Underleverandør som på vegne av Databehandler utfører oppgaver i forbindelse med ytelser til Behandlingsansvarlig, herunder oppdrag der overføring og/eller behandling av personopplysningene inngår, skal være gjort kjent med og avtalemessig forpliktet seg til Databehandlers avtalemessige og lovmessige forpliktelser og skal opptre i samsvar med disse.

Databehandler er ansvarlig for å ha en oversikt over hvilke underleverandører det er samtykket til å benytte i forbindelse med sin leveranse av ytelser til Behandlingsansvarlig i **vedlegg 2**. Oversikten skal inneholde angivelse av lokasjon/driftssted for utførelsen, angi hvilke tjenester/oppgaver som utføres og angi om det overføres personopplysninger eller taushetsbelagte opplysninger til underleverandøren. Også eventuelle endringer i lokasjon/driftssted og i bruk av underleverandører forutsetter skriftlig samtykke fra Behandlingsansvarlig.

Databehandler er ansvarlig for underleverandørens utførelse av oppgaver for Behandlingsansvarlig, på samme måte som om Databehandler sto for utførelsen selv.

Krav om forhåndssamtykke fra Behandlingsansvarlig gjelder også de tilfeller der Databehandler og/eller underleverandørers behandling omfatter overføring av personopplysninger til land utenfor EU/EØS (tredjeland). Slik overføring forutsetter gyldig overføringsgrunnlag i samsvar med Databehandleravtalen.

Samtykker til at oppdrag/oppgaver utføres av underleverandører eller endringer i lokasjon/driftssted, skal tilknyttes Databehandleravtalen ved endringsavtale, som dokumenterer grunnlaget for samtykke.

5. Sikkerhet

Databehandler skal oppfylle de krav til sikkerhetstiltak som stilles etter det til enhver tid gjeldende personvernregelverk, jf. GDPR kapittel 4. Databehandler skal dokumentere rutiner og andre tiltak for å oppfylle disse kravene. Dokumentasjonen skal være tilgjengelig på behandlingsansvarliges forespørsel.

Databehandleren skal sørge for at tilfredsstillende informasjonssikkerhet er etablert gjennom planlagte og systematiske tiltak. I den forbindelse skal Databehandler oversende dokumentasjon til Behandlingsansvarlig om mål og strategi for informasjonssikkerheten, dersom Behandlingsansvarlig ber om dette.

Databehandler plikter å gi behandlingsansvarlig tilgang til sin sikkerhetsdokumentasjon, og bistå, slik at behandlingsansvarlig kan ivareta sitt eget ansvar etter gjeldende personvernregelverk. Databehandleren må tilgjengeliggjøre all informasjon og dokumentasjon som er nødvendig for å påvise at forpliktelsene etter denne Avtale er oppfylt. Om sikkerhetsnivået ikke er tilfredsstillende, plikter Databehandler å justere sikkerhetsnivået etter instruks fra Behandlingsansvarlig.

Databehandler skal underrette Behandlingsansvarlig om avvik uten ugrunnet opphold og senest innen 24 timer etter at Databehandler fikk mistanke om avviket, selv om Databehandler ikke har all påkrevet informasjon tilgjengelig.

Behandlingsansvarlig har ansvaret for den videre håndtering av bruddet, herunder for at Datatilsynet blir underrettet, uten ugrunnet opphold og, når det er mulig, senest 72 timer etter å ha fått kjennskap til avviket.

6. Sikkerhetsrevisjoner

Databehandler har et selvstendig ansvar for og skal oppfylle krav til tekniske og organisatoriske sikkerhetstiltak som stilles etter denne Databehandleravtale for å oppnå egnet personopplysningssikkerhet. Det vises særlig til GDPR artikkel 28 og 32-36.

Behandlingsansvarlig har rett til selv eller ved en tredjepart godkjent av Databehandler, å revidere Databehandlers personopplysningssikkerhet. Slike revisjoner skal kunne gjennomføres i rimelig tid etter skriftlig forhåndsvarsel fra Behandlingsansvarlig. Revisjonen kan omfatte gjennomgang av rutiner, stikkprøvekontroller, mer omfattende stedlige kontroller og andre egnede kontrolltiltak. Databehandler plikter å muliggjøre og bidra til revisjon og inspeksjon som gjennomføres av eller på vegne av Behandlingsansvarlig. De som utfører revisjon må imidlertid forholde seg til Databehandlers rimelige instruksjoner ved adgang til Databehandlers lokaler og for øvrig akseptere Databehandlers saklige behov for konfidensialitet. Databehandlers deltakelse på revisjoner er kostnadsfri. Databehandler kan likevel fakturere Behandlingsansvarlig for sine kostnader ved bistand og medvirkning til revisjonen i den grad arbeidet overstiger hva loven krever.

7. Avtalens varighet

Avtalen gjelder så lenge Databehandler behandler personopplysninger på vegne av Behandlingsansvarlig.

Avtalen trer i kraft ved signering. For det tilfellet at Databehandler har behandlet personopplysninger på vegne av Behandlingsansvarlig forut for inngåelse av Avtalen, skal Avtalen få anvendelse også for disse forutgående forholdene.

Ved brudd på denne Avtale eller brudd på gjeldende personvernregelverk kan Behandlingsansvarlig pålegge Databehandler å stoppe den videre behandlingen av opplysningene med øyeblikkelig virkning.

Dersom brudd på denne Databehandleravtale ikke rettes innen rimelig tid, kan Behandlingsansvarlig si opp Databehandleravtalen helt eller delvis etter forutgående skriftlig varsel. Ved helt eller delvis opphør av denne Databehandleravtale, vil ytelser etter andre avtaler mellom partene som er knyttet til denne Databehandleravtale også opphøre i den utstrekning de omfatter behandling av personopplysninger.

8. Ved opphør

Avtalen kan fritt sies opp av Behandlingsansvarlig med en frist på 3 måneder. Databehandler kan si opp Avtalen med 1 måneds varsel dersom Behandlingsansvarlig er i gjentatt mislighold av sine forpliktelser overfor Databehandler.

Ved opphør av Databehandleravtalen mellom partene, plikter Databehandler etter Behandlingsansvarliges nærmere instruksjon å tilbakelevere, overføre, slette og/eller forsvarlig destruere alle personopplysninger som er behandlet på vegne av den Behandlingsansvarlige og som omfattes av denne Databehandleravtalen, med mindre annet er spesifisert i vedlegg 1. Dette omfatter også sletting av logger, sikkerhetskopier og lignende, som Databehandler ikke selv har behandlingsgrunnlag for å oppbevare. Databehandler skal fremlegge skriftlig

dokumentasjon på at ovennevnte krav er oppfylt. Behandlingsansvarlig har rett til revisjon etter punkt 6, gjelder også etter opphør av Databehandleravtalen.

Plikten til overføring omfatter overføring til Behandlingsansvarlig og/eller en annen databehandler, slik at kontinuitet i Behandlingsansvarliges virksomhet ikke påvirkes.

Databehandleren kan imidlertid fritas fra plikten til å slette dersom norsk lov krever at opplysningene fortsatt skal lagres. I alle tilfelle skal opplysningene tilbakeleveres eller slettes samtidig som oppbevaringsplikten opphører.

9. Meddelelser

Meddelelser etter denne avtalen skal sendes skriftlig til

For Behandlingsansvarlig: Janne Havdal Nordbø, janne.nordbo@rennebu.kommune.no

For Databehandler: Eivind Olsen, (seksjonssjef), eivind.olsen@prokom.no

10. Lovvalg og verneting

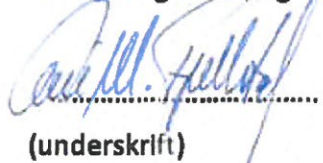
Avtalen er underlagt norsk rett og partene vedtar Oslo tingrett som verneting. Dette gjelder også etter opphør av avtalen.

11. Undertegning

Denne avtale er i 2 – to eksemplarer, hvorav partene har hvert sitt.

Rennebu kommune 20.02.2020

Behandlingsansvarlig



(underskrift)

Databehandler



(underskrift)

Vedlegg:

1. Oversikt over personopplysninger som omfattes av denne databehandleravtalen
2. Oversikt og beskrivelse av underleverandører

Vedlegg 1 til databehandleravtale

Oversikt over personopplysninger i BookUp

Formålet med behandlingen

BookUp er et system for utleie av idrettsbaner, selskapslokaler og egentlig alt som kan leies ut. Brukerne avgir personinformasjon som er nødvendig for behandlingsansvarliges behandling av søknaden/forespørselen.

Type personopplysninger som behandles

BRUKERPROFIL – Epost-adressen benyttes som unik identifikator i systemet.

KONTOINFORMASJON – Benyttes av utleier for å avgjøre om leietaker har krav på ulike utleievilkår. Informasjonen benyttes også videre i en ev. faktureringsprosess. Denne kan enten være personlig, direkte knyttet mot brukerprofil, eller være på vegne av forening/aktør som er knyttet mot flere brukerprofiler.

METADATA – Benyttes for å knytte leietidspunkt opp mot ansvarlig leietaker.

BookUp er satt opp med Google Analytics for statistikkformål. Her samles inn informasjon om bla. nettleser, språkinnstilling, device etc. Se for øvrig Googles [Personvern og sikkerhet for data for Google Analytics](#).

Behandlingens art

INNSAMLING OG LAGRING

Brukerprofil og kontoinformasjon opprettes ved første gangs bruk av systemet. Og kan videre vedlikeholdes via innebygd løsning for Min Konto ved behov.

Utleier har mulighet til å registrere bankkonto-nummer for å motta direkte betaling via kort. Navn og adresse tilknyttet denne kontoen blir også lagret.

Betaling utført direkte i løsningen via debit- eller kredittkort gjøres via betalingsløsningen Stripe (<https://stripe.com/no>).

OVERFØRING TIL FAKTURASYSTEM

Informasjon om booking oversendes kundens infrastruktur via sikker linje.

Varighet av behandlingen

BRUKERPROFIL – Lagres inntil brukeren selv velger å slette sin profil.

KONTOINFORMASJON – Lagres inntil brukeren selv velger å slette sin informasjon. Merk at kontoinformasjon ikke kan slettes før aktive bookinger er avsluttet.

METADATA – Ligger tilknyttet booking-tidspunkt inntil disse ev. slettes.

Innsyn i egne personopplysninger

Bruker kan etter innlogging selv sjekke hvilke opplysninger som er registrert om ham/henne.

Rett til å bli glemt

Tjenesten har "Glem meg"-funksjonalitet som gir brukeren mulighet for å slette egen brukerprofil med alle tilhørende data.

Personvernerklæring

BookUp presenterer en personvernerklæring som brukeren må godkjenne for å benytte løsningen.

Vedlegg 2 til databehandleravtale

Oversikt og beskrivelse av underdatabehandlere for BookUp

Løsningen driftes ved kjøpsavtalens inngåelse av følgende underdatabehandler:

- Microsoft Azure – Microsoft Corporation

Driftslokasjon

- Underdatabehandler benytter p.t. servere i EU, nærmere bestemt Irland og Tyskland.