DATABEHANDLERAVTALE

Mellom

Gripr AS, org. Nr 918 889 450 MVA («**Databehandler**»)

og

[KUNDEN], org. nr. [xxx xxx xxx] («**Behandlingsansvarlig**»)

er avtale om behandling av personopplysninger («**Avtalen**») som Databehandler skal foreta for Behandlingsansvarlig som følge av avtale inngått med Databehandleren som Leverandør og Behandlingsansvarlige som Kunde av [dato].

1. Avtalens formål

Databehandler behandler personopplysninger på vegne av Behandlingsansvarlig på den bakgrunn som følger ovenfor.

Formålet med behandlingen, varigheten av behandlingen, behandlingens art, de typer personopplysninger som skal behandles og kategorier av registrerte følger av vedlegg til Avtalen.

Avtalen skal sikre at personopplysninger behandles i samsvar med de til enhver gjeldende kravene til behandling av personopplysninger, herunder bl.a. EU-direktiv 95/46/EF av 24. oktober 1995 om beskyttelse av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger som er implementert i Norge ved lov av 14. april 2000 nr. 31 om behandling av personopplysninger (personopplysningsloven) med tilhørende forskrifter, samt kravene etter Europaparlaments- og rådsforordning om beskyttelse av individer ved behandling av personopplysninger og om fri flyt av slike opplysninger og om oppheving av direktiv 95/46/EF (personvernforordningen) som besluttet 27. april 2016, og norsk lov med tilhørende forskrifter som innføres som en følge av personvernforordningen og erstatter personopplysningsloven (i det følgende er både dagens og ny personopplysningslov omtalt som «personopplysningsloven»).

Databehandler skal behandle personopplysningene på den måte som er beskrevet i Avtalen, samt på annen måte dersom dette er skriftlig avtalt mellom Databehandleren og Behandlingsansvarlig.

Begreper og definisjoner benyttet i Avtalen skal forstås på samme måte som i personopplysningsloven.

2. Behandlingsansvarliges rettigheter og plikter. Databehandlers plikter

Databehandleren bekrefter at denne vil gjennomføre egnede tekniske og organisatoriske tiltak som sikrer at all behandling under denne Avtalen oppfyller kravene i personopplysningsloven og vern av den registrertes rettigheter, herunder innfrir alle kravene etter personvernforordningens artikkel 32. Se også ytterligere plikter i punkt 4. Den behandlingsansvarlig skal til enhver tid ha full rettslig rådighet over personopplysningene.

Databehandleren skal bare behandle personopplysningene basert på dokumenterte instrukser fra den Behandlingsansvarlige. Databehandleren skal til enhver tid kunne dokumentere slike instrukser. Databehandler skal ikke behandle personopplysninger Databehandleren får tilgang til på annen måte enn det som er nødvendig for å utføre de oppdrag som Databehandler har for den Behandlingsansvarlige.

Databehandleren skal bistå den Behandlingsansvarlige i å svare på anmodninger som den registrerte inngir med henblikk på å utøve sine rettigheter etter personvernforordningens kapittel III hensyntatt behandlingens art og i den grad det er mulig, bistår, ved hjelp av egnede tekniske og organisatoriske tiltak, samt bistå den Behandlingsansvarlige med å sikre overholdelse av forpliktelsene knyttet til personopplysningssikkerhet og vurdering av personvernkonsekvenser og forhåndsdrøftinger i personvernforordningens artikkel 32 til 36, hensyntatt behandlingens art og den informasjonen som er tilgjengelig for Databehandleren. Foreligger det godkjente adferdsnormer etter personvernforordningens artikkel 40 eller godkjent sertifiseringsordning etter artikkel 42, som Databehandleren har påtatt seg å overholde eller være sertifisert etter, plikter Databehandleren å etterkomme slike adferdsnormer eller sertifiseringskrav.

Databehandleren skal føre protokoll (logg) over behandlingsaktiviteter denne utfører på vegne av den Behandlingsansvarlige, som skal inneholde minimum den informasjon som er pålagt etter personvernforordningen artikkel 30. Den Behandlingsansvarlige kan til enhver tid kreve oversendt kopi av slik protokoll.

Databehandleren skal gjøre tilgjengelig for den Behandlingsansvarlige all informasjon som er nødvendig for å påvise at forpliktelsene fastsatt i denne dette punkt 2 er oppfylt, samt muliggjøre og bidra til revisjoner, herunder inspeksjoner, som gjennomføres av den Behandlingsansvarlige eller en annen inspektør på fullmakt fra den Behandlingsansvarlige. Dette omfatter også å gi tilgang til sikkerhetsdokumentasjon. Den Behandlingsansvarlige har selv det direkte ansvaret overfor aktuelle tilsynsmyndigheter.

Databehandleren har taushetsplikt om personopplysninger som vedkommende får tilgang til som en følge av Avtalen og behandling av personopplysningene, og skal sikre at personer som er autorisert til å behandle personopplysningene, har forpliktet seg til å behandle opplysningene fortrolig eller er underlagt en egnet lovfestet taushetsplikt. Denne bestemmelsen gjelder også etter Avtalens opphør.

Databehandleren skal ikke utlevere opplysninger eller informasjon som denne behandler for den Behandlingsansvarlige til tredjepart uten eksplisitt pålegg fra den Behandlingsansvarlige. Henvendelser til Databehandleren skal Databehandleren videreformidle til Behandlingsansvarlige så raskt som mulig.

Er Databehandleren av den oppfatning at en instruks fra den Behandlingsansvarlige er i strid med personvernforordningen, personopplysningsloven, eller annen regulering av behandling av personopplysninger, skal Databehandleren umiddelbart underrette den Behandlingsansvarlige om dennes oppfatning. Databehandleren plikter å utøve sine plikter etter Avtalen til tross for sin oppfatning.

3. Bruk av underleverandør

Databehandleren skal kun benytte underleverandører til behandling av personopplysninger (underdatabehandler) som er skriftlig godkjent av den Behandlingsansvarlige og som har bekreftet å gjennomføre egnede tekniske og organisatoriske tiltak som sikrer at all behandling under denne Avtalen oppfyller kravene i personopplysningsloven og vern av den registrertes rettigheter.

Godkjente underdatabehandlere ved Avtalens inngåelse er spesifisert i vedlegg 1 til Avtalen.

Behandlingsansvarlig gir Databehandleren generell tillatelse til bruk av underdatabehandler for behandling av personopplysninger etter Avtalen. I tilfelle har planer om å benytte andre underdatabehandlere eller skifte ut underdatabehandlere, skal Databehandleren underrette den

Behandlingsansvarlige om planene og dermed gi den Behandlingsansvarlige muligheten til å motsette seg slike endringer.

Underdatabehandler skal være gjort kjent med Databehandlerens forpliktelser etter denne Avtalen og regelverket som regulerer behandling av Behandlingsansvarliges personopplysninger, og skal pålegges de samme forpliktelsene med hensyn til vern av personopplysninger som er fastsatt i Avtalen hvor underdatabehandler skal gi tilstrekkelige garantier for at det vil bli gjennomført tekniske og organisatoriske tiltak som sikrer at behandlingen oppfyller lovmessige krav. Dersom underdatabehandler ikke oppfyller sine forpliktelser med hensyn til vern av personopplysninger og kravene i Avtalen, skal Databehandleren overfor den Behandlingsansvarlige ha fullt ansvar for at underdatabehandler oppfyller sine forpliktelser.

4. Sikkerhet og avvik

Databehandleren skal oppfylle de krav til sikkerhetstiltak som stilles etter personopplysningsloven med forskrifter. Databehandleren skal kunne dokumentere rutiner og andre tiltak for å oppfylle disse kravene. Dokumentasjonen skal være tilgjengelig på den Behandlingsansvarliges forespørsel.

Det skal gjennomføres sikkerhetsrevisjoner jevnlig, og partene skal avtale seg imellom tidspunkter for sikkerhetsrevisjoner. Revisjonen kan omfatte gjennomgang av rutiner, stikkprøvekontroller, mer omfattende stedlige kontroller og andre egnede kontrolltiltak. Det skal avtales den Behandlingsansvarliges plikt til å dekke eventuelle ressursforbruk forbundet med utøvelse av slik revisjon.

I tilfelle sikkerhets- eller personvernbrudd, skal Databehandleren varsle den Behandlingsansvarlige uten ugrunnet opphold. Melding om brudd skal minimum inneholde:

1. Beskrivelse av 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 personopplysningsposter som er berørt,

2. navnet på og kontaktopplysningene til personvernrådgiveren eller et annet kontaktpunkt der mer informasjon kan innhentes,

3. beskrivelse av de sannsynlige konsekvensene av bruddet på personopplysningssikkerheten,

4. beskrivelse av de tiltak som er truffet eller foreslår å treffe for å håndtere bruddet på personopplysningssikkerheten, herunder, dersom det er relevant, tiltak for å redusere eventuelle skadevirkninger som følge av bruddet.

Dersom ikke alle opplysninger kan gis i første melding, skal opplysningene gis suksessivt så snart de foreligger.

Den Behandlingsansvarlige har ansvaret for å sende melding til tilsynsmyndighet, og Databehandler skal ikke sende slik melding eller kontakte tilsynsmyndighet uten at den Behandlingsansvarlige har gitt instruks om dette.

5. Overføring til utlandet

Personopplysninger skal kun overføres til land utenfor EU/EØS (tredjeland) etter instruks fra den Behandlingsansvarlige. Databehandleren skal altså ikke overføre eller la personer i tredjeland på noen måte få tilgang til personopplysninger uten at Behandlingsansvarlig har eksplisitt godkjent

dette skriftlig og gitt instruks om overføring eller tilgang på forhånd. Samtykke og instruks må dekke hvilke land opplysningene skal kunne overføres til. Overføring til tredjeland forutsetter, selv med samtykke og instruks, at de krav til sikkerhet og vern av de registrertes rettigheter som følger av personopplysningsloven og annet regelverk er ivaretatt.

6. Avtalens varighet, pålegg om stans, plikter ved opphør/oppsigelse

Avtalen gjelder så lenge Databehandleren behandler eller har tilgang til personopplysninger på vegne av Behandlingsansvarlige etter Hovedavtalen.

Ved brudd på denne Avtalen, personopplysningsloven eller annet relevant regelverk, kan Behandlingsansvarlige pålegge Databehandleren å stoppe den videre behandlingen av opplysningene med øyeblikkelig virkning.

Databehandleren skal, etter den Behandlingsansvarliges instruksjon, slette eller tilbakelevere alle personopplysninger til den Behandlingsansvarlige etter at tjenestene knyttet til behandlingen er levert, og sletter eksisterende kopier, med mindre det er et lovmessig krav om at personopplysningene skal fortsatt lagres. Dette gjelder også for eventuelle sikkerhetskopier, men hvor det er tilstrekkelig med å overskrive etter de etablerte rutiner for sikkerhetskopiering.

Den Behandlingsansvarlige skal motta en skriftlig bekreftelse fra Databehandleren på at alle personopplysninger er returnert eller slettet i henhold til den Behandlingsansvarliges instruksjoner og at Databehandleren ikke har beholdt kopi, utskrifter eller andre former for personopplysninger i noen form.

7. Øvrige plikter og rettigheter

Øvrige plikter og rettigheter følger av Hovedavtalen som gjelder mellom Databehandleren og Behandlingsansvarlige om tjenestene som nødvendiggjør behandling av personopplysninger og denne Avtale. De samme kontaktpersoner gjelder for Avtalen som etter Hovedavtalen.

Denne Avtalen skal ikke utvide Behandlingsansvarliges sanksjonsmuligheter, herunder erstatningsansvar for Databehandleren, utover det som følger av Hovedavtalen.

Ved eventuell overdragelse av Hovedavtalen til andre parter, skal denne Avtale overdras tilsvarende.

8. Meddelelser

Meddelelser etter denne Avtalen skal sendes skriftlig til: hjelp@gripr.no

9. Lovvalg og verneting

Avtalen er underlagt norsk rett og partene vedtar Sandefjord tingrett som verneting. Dette

gjelder også etter opphør av Avtalen.

DATO FOR AVTALE AKSEPT

Databehandler	**Behandlingsansvarlig**
Kim André Heggenes-Ulleland (sign)	Signer her (sign)
GRIPR AS	KUNDENAVN

Vedlegg

Formålet med behandlingen

Etter Hovedavtalen skal Behandligsansvarlig bruke tjenester levert av Databehandler hvor formålet er å gjøre virksomheten mer digital og effektiv. For å gjøre dette flyttes store deler av virksomhetens oppgaver over til skybasert software hvor virksomheten kan styre og utføre de daglige oppgavene på nett. De ansatte (også kalt brukere) har tilgang til å utføre en rekke tjenester på nett for å gjøre arbeidet enklere.

Varigheten av behandlingen

Behandlingen som nevnt i denne avtalen skal vare så lenge Databehandler yter tjenester etter Hovedavtalen til Behandlingsansvarlig.

Behandlingens art

Lagring og oppbevaring av personopplysninger

Typer personopplysninger som skal behandles

Følgende personopplysninger skal behandles under Avtalen:

Opplysninger som ofte behandles er:

- Navn

- Adresse, postnummer og poststed

- Telefonnummer

- E-postadresse

- Profilbilde

Kategorier av registrerte

Følgende kan registreres og behandles:

- Ansatte
- Leverandører
- Kunder

Underdatabehandlere ved inngåelse av Avtalen

Se vedlegg

Oversikt over alle IT-Leverandører

Cosmos IT:

- Dette er en av våre serverleverandører hvor all data lagres og oppbevares i trygge og sikre omgivelser.
- Data som lagres er navn, mobilnummer, e-postadresse og ansattnummer.

Microsoft Azure:

- Dette er en av våre serverleverandører hvor all data lagres og oppbevares i trygge og sikre omgivelser.
- Data som lagres er navn, mobilnummer, e-postadresse og ansattnummer.

Tray.io:

- Gripr AS har integrasjoner mot Tray.io hvor det sendes data relatert til prosjekter, kunder, oppgaver, dokumenter og brukere.
- Data som sendes er: Brukernavn, prosjekter, kunder, oppgaver og filer.

- Tray.io er integrert med følgende systemer hvor data deles:
    - Boligmappa

Productboard:

- Dette er vår planleggingsverktøy hvor vi kan motta forespørsler fra våre kunder om ønsket funksjonalitet. I den forbindelser lagres opplysninger som e-post, navn og firmanavn.

Stonly:

- Dette er vårt verktøy hvor vi lager hjelperartikler som våre kunder kan lese for å få hjelp. I noen tilfeller kan vi lage guides som trigges av spesielle data properties og i den forbindelse så tracker vi data som: brukerrolle, domene (kan være firmanavn), språk, når en bruker sist har vært aktiv.

Segment:

- Dette er vårt analyse verktøy som er integrert med gripr.io for å tracke alle hendelser som foregår i vår programvare. Dette er for at vi skal kunne forbedre vår funksjonalitet for å kunne tilby en bedre programvare. I den forbindelse så tracker vi e-post, navn, firma samt alle eventer når noe blir laget, endret eller slettet i gripr.io.

SendGrid:

- Dette er vårt verktøy for å sende ut e-poster til våre kunder når noe skjer i gripr.io, men det lagres ingen data for at dette skal fungere. Her kan hver enkelt bruker selv avgjøre om man ønsker varslinger.

OneSignal:

- Dette er vårt verktøy for å kunne sende ut push varslinger i vår native applikasjon. For å sende ut varslinger må vi lagre data som e-post for å kunne identifisere hvem som skal ha varsel.

Hubspot:

- Hubspot er vårt CRM verktøy hvor alle opplysninger om våre kunder og brukere lagres. Her lagres det en rekke opplysninger som gir oss den informasjon vi trenger for kunne opprettholde en god kunderelasjon, tilby vår programvare og utføre kundesupport når det er behov. Hvilke opplysninger som lagres kan få på etterspørsel.

Master Regnskap:

- Dette er Gripr AS sin egen regnskapsfører og i den forbindelse blir det fakturert ut mot kunde hvor enkelt opplysninger blir nevnt i faktura sammenheng.
- Data som brukes er virksomhetens navn, adresse, postnummer, poststed, telefon og e-post samt navn på kontaktperson/referanse.

All behandling av personopplysninger som vi foretar skjer innenfor EU/EØS-området.

Vedlegg 2

Tekniske beskrivelse

1. Tilgang til data
    a. Tilgang til data er kun tilgjengelig for Teknisk ansvarlig og Daglig leder i GRIPR AS hvor disse er underlagt taushetsplikt ovenfor den data som er tilgjengelig.
    b. Teknisk ansvarlig er Jørgen Rudolph Låker
    c. Daglig leder er Kim Andre Heggenes-Ulleland

2. Lagring av data
    a. Oppbevaring og lagring av data er samlet i en database i PostgreSQL. Hver kunder har sin unike UID med tilhørende mekanismer som sørger for at det kun er relevant data som gjøres tilgjengelig.
    b. Lagring av data for GRIPR filbehandler er lagret i en og samme Database som er hostet på Microsoft Azure. Data er her lagret med relasjon til bruker og domene, i tillegg til at det genereres en unik UID, på den måten er data kun tilgjengelig for hvert enkelt domene og det vil være umulig å få tilgang til data relatert til et annet domene.

3. Server oppsett
    a. Servere er definert og stilt inn på den metoden som gir kunden den beste sikkerheten og tryggheten mot databrudd, inntrengere og nedetid.
    b. Servere er delt opp i 3 lag
        i. Lag 1 – Server for websiden som er synlig for kunden på internett
        ii. Lag 2 – Server for applikasjon som lar kunden bruke systemet. Her ligger det en brannmur mellom lag 1 og 2.
        iii. Lag 3 – Server for oppbevaring av data som er begrenset slik at applikasjonen i lag 2 med sin unike IP-Adresse er den eneste som kan få tilgang til Lag 3.

4. Backup
    a. Det er satt opp en service som utfører en backup av kundens database som inneholder av lagret data til faste tider som utføres 1 gang pr døgn.
    b. Backup innehar en system recover funksjon som lar oss gjenopprette all data innen rimelig tid som er ca max 30 min.

5. Feilsøking
    a. Ved en feil som blir rapportert fra kunde eller internt er første trinn å gjenskape feilen på lokale-test servere som er uavhengige fra kundens systemer.
    b. Når feilen er gjenskapt utfører man en analyse for å isolere hva som er feil og hvor feilen ligger i systemet.
    c. Når feilen er avdekket så blir feilen utbedret på lokale-test servere i utviklingsmiljøet, hvor det blir utført tester som sikrer at feilen er utbedret.
    d. Kunden blir informert via interne meldingssystemer om at feilen er avdekket og fikset og man blir enige om tidspunkt for å pushe fiks til live server.
    e. Når fiksen er pushet blir det i tillegg utført en test på live servere for å kvalitetssikre at feilen er fikset og fungerer som den skal.

6. Data på avveie

a. Skulle data komme på avveie blir det raskt tatt en vurdering av omfanget, alle berørte kunder og personer blir varslet og berørte servere ved høy risiko stenges for å hindre videre brudd.
b. Ved risiko for de registrerte sine rettigheter og friheter varsles Datatilsynet innen 72 timer om hva som har skjedd ved bruk av vårt utarbeidet avviksskjema for disse tilfeller.
c. Det vil bli gjort en analyse for å avdekke hvilken data som er på avveie slik at tiltak kan utføres så raskt som mulig.