Databehandleravtale

I henhold til gjeldende norsk personopplysningslovgivning og forordning (EU) 2016/679 av 27. april 2016, Artikkel 28 og 29, jf. Artikkel 32-36, inngås følgende avtale

mellom

{{firmanavn}}, Org. nr. {{orgnr}}

(behandlingsansvarlig)

og

Tappin AS, Org. nr. 999215777

(databehandler)

Begrep som benyttes i avtalen følger enten naturlig språklig forståelse, defineres i avtalen, eller leses slik de er definert i forordning (EU) 2016/679 av 27. april 2016, Artikkel 4.

1. Avtalens hensikt

Partene til denne Databehandleravtalen har inngått en avtale av 01.06.21 ("**Avtalen**") på bakgrunn av kjøp av arrangementsteknisk bistand. Denne Databehandleravtalen regulerer partenes rettigheter og forpliktelser for å sikre at all behandling av personopplysninger skjer i henhold til gjeldende lovgivning om behandling av personopplysninger, herunder EUs personvernforordning 2016/679 ("**GDPR**") og i gjeldende personvernlovgivning som gjennomfører denne («**personopplysningslovgivningen**»).

Databehandleravtalen skal sikre at personopplysninger ikke brukes ulovlig, urettmessig eller at opplysningene behandles på måter som fører til uautorisert tilgang, endring, sletting, skade, tap eller utilgjengelighet.

Databehandleravtalen regulerer databehandlers forvaltning av personopplysninger på vegne av den behandlingsansvarlige, herunder innsamling, registrering, sammenstilling, lagring, prosessering, utlevering og sletting eller kombinasjoner av disse, i forbindelse med bruk av/behandling i arrangementsteknisk bistand (heretter omtalt som "**tjenesten**").

Ved motstrid skal vilkårene i denne avtalen gå foran databehandlers personvernerklæring eller vilkår i andre avtaler inngått mellom behandlingsansvarlig og databehandler i forbindelse med bruk av/behandling i tjenesten.

2. Behandlingens formål

Formålet med databehandlers forvaltning av personopplysninger på vegne av behandlingsansvarlig, er arrangementsteknisk bistand.

Personopplysninger som databehandler forvalter på vegne av behandlingsansvarlig kan ikke brukes til andre formål uten at dette på forhånd er godkjent av behandlingsansvarlig.

Databehandler kan ikke overføre personopplysninger som omfattes av denne avtalen til samarbeidspartnere eller andre tredjeparter uten at dette på forhånd er godkjent av behandlingsansvarlig, jf. punkt 10 i denne avtalen.

3. Instrukser

Behandlingsansvarlig har, som ansvarlig for at personopplysningene blir behandlet i samsvar med personvernlovgivningen, rett og plikt til å bestemme hvilke formål som skal gjelde og hvilke hjelpemidler som skal benyttes i behandlingen.

Behandlingsansvarlige skal gi databehandleren dokumenterte instrukser for hvordan personopplysninger skal behandles. Dersom ingen andre instrukser blir gitt, utgjør denne databehandleravtalen de gjeldende instruksene.

Databehandler skal bare behandle personopplysninger etter skriftlig instruks fra behandlingsansvarlig og skal følge de dokumenterte instruksene for forvaltning av personopplysninger i tjenesten som behandlingsansvarlig har bestemt skal gjelde.

Databehandler skal protokollføre alle behandlingsaktiviteter og overholde alle plikter i henhold til gjeldende norsk personopplysningslovgivning som gjelder ved bruk av tjenesten til behandling av personopplysninger.

Databehandler forplikter seg til å varsle behandlingsansvarlig dersom databehandler mottar instrukser fra behandlingsansvarlig som databehandleren mener er i strid med bestemmelsene i gjeldende norsk personopplysningslovgivning.

Databehandler skal på forespørsel bistå behandlingsansvarlig med å utføre en personvernkonsekvensvurdering, også kjent som en "Data Protection Impact Assessment". Databehandler skal på samme måte etter anmodning bistå med å sikre at krav til innebygd personvern i databehandlers løsninger innfris. Dette inkluderer å bygge inn funksjonalitet for å oppfylle personvernprinsipper samt funksjonalitet for å sikre den registrertes rettigheter, så langt det med rimelighet kan forventes med hensyn til formålet med løsningen.

Databehandler skal påse at personopplysninger som behandles på vegne av behandlingsansvarlig holdes fysisk eller logisk atskilt fra andre data som databehandler behandler.

4. Registrerte og opplysningstyper

Databehandler vil behandle personopplysninger i den utstrekning det er nødvendig for å oppfylle Avtalen. Kategorier av personopplysninger og kategorier av registrerte personer er spesifisert i **Bilag 1.**

5. De registrertes rettigheter

Databehandler plikter å bistå behandlingsansvarlig ved ivaretakelse av den registrertes rettigheter i henhold til gjeldende norsk personopplysningslovgivning.

Den registrertes rettigheter inkluderer retten til informasjon om hvordan hans eller hennes personopplysninger behandles, retten til å kreve innsyn i egne personopplysninger, retten til å kreve retting eller sletting av egne personopplysninger og retten til å kreve at behandlingen av egne personopplysninger begrenses.

I den grad det er relevant, skal databehandler bistå behandlingsansvarlig med å ivareta de registrertes rett til dataportabilitet og retten til å motsette seg automatiske avgjørelser, inkludert profilering.

6. Tilfredsstillende informasjonssikkerhet

Databehandler skal iverksette tilfredsstillende tekniske, fysiske og organisatoriske sikringstiltak for å beskytte personopplysninger som omfattes av denne avtalen mot uautorisert eller ulovlig tilgang, endring, sletting, skade, tap eller utilgjengelighet.

Databehandler skal dokumentere egen sikkerhetsorganisering, retningslinjer og rutiner for sikkerhetsarbeidet, risikovurderinger og etablerte tekniske, fysiske eller organisatoriske sikringstiltak. Dokumentasjonen skal være tilgjengelig for behandlingsansvarlig på forespørsel.

Databehandler skal etablere kontinuitets- og beredskapsplaner for effektiv håndtering av alvorlige sikkerhetshendelser. Dokumentasjonen skal være tilgjengelig for behandlingsansvarlig på forespørsel.

Databehandler skal gi egne ansatte tilstrekkelig informasjon om og opplæring i informasjonssikkerhet slik at sikkerheten til personopplysninger som behandles på vegne av behandlingsansvarlig blir ivaretatt.

En detaljert beskrivelse av tiltak for informasjonssikkerhet vedlegges i **Bilag 2.**

7. Taushetsplikt

Kun ansatte hos databehandler som har tjenstlige behov for tilgang til personopplysninger som forvaltes på vegne av behandlingsansvarlig, kan gis slik tilgang. Databehandler plikter å dokumentere retningslinjer og rutiner for tilgangsstyring. Dokumentasjonen skal være tilgjengelig for behandlingsansvarlig på forespørsel.

Databehandler og de ansatte hos databehandler har konfidensialitets- og taushetsplikt om dokumentasjon og personopplysninger som vedkommende får tilgang til i henhold til denne avtalen. Konfidensialitets- og taushetsplikten omfatter tredjeparter og deres ansatte som utfører oppdrag som underdatabehandler eller utfører vedlikehold (eller liknende oppgaver) av systemer, utstyr, nettverk eller bygninger som databehandler anvender for å levere tjenesten. Konfidensialitets- og taushetspliktene gjelder også etter Avtalens opphør.

Databehandler plikter å dokumentere at de som her er pålagt taushetsplikt har mottatt informasjon om taushetsplikten og samtykket til å være bundet av denne. Dokumentasjonen skal være tilgjengelig for behandlingsansvarlig på forespørsel.

Norsk lov vil kunne begrense omfanget av taushetsplikten for ansatte hos databehandler og tredjeparter.

8. Tilgang til informasjon og sikkerhetsdokumentasjon

Behandlingsansvarlig har, med mindre annet er avtalt eller følger av lov, rett til tilgang til og innsyn i personopplysningene som databehandleren håndterer og de systemene som benyttes til dette formål. Databehandler skal på forespørsel gjøre tilgjengelig for behandlingsansvarlig de behandlede personopplysningene og all informasjon om

behandlingen som er nødvendig for å påvise om partenes forpliktelser er oppfylt eller ikke. Databehandler plikter å gi nødvendig bistand i denne forbindelse.

Databehandler plikter på forespørsel å gi behandlingsansvarlig tilgang til all sikkerhetsdokumentasjon som er nødvendig for at behandlingsansvarlig skal kunne ivareta sine forpliktelser i henhold til gjeldende norsk personopplysningslovgivning, samt å samarbeide med behandlingsansvarlig og tilsynsmyndigheten i denne forbindelse.

Behandlingsansvarlig har taushetsplikt for konfidensiell sikkerhetsdokumentasjon som databehandler gjør tilgjengelig for behandlingsansvarlig.

9. Varslingsplikt ved sikkerhetsbrudd

Databehandler skal uten ugrunnet opphold varsle behandlingsansvarlig dersom personopplysninger som forvaltes på vegne av behandlingsansvarlig utsettes for sikkerhetsbrudd.

Varselet til behandlingsansvarlig skal som minimum inneholde informasjon som beskriver sikkerhetsbruddet, hvilke registrerte som er berørt av sikkerhetsbruddet, hvilke personopplysninger som er berørt av sikkerhetsbruddet, hvilke strakstiltak som er iverksatt for å håndtere sikkerhetsbruddet og hvilke forebyggende tiltak som eventuelt er etablert for å unngå liknende hendelser i fremtiden.

Behandlingsansvarlig er ansvarlig for at Datatilsynet blir varslet når dette er påkrevd.

10. Underleverandører

Databehandler plikter før behandlingen av personopplysninger starter å inngå egne avtaler med underleverandører som regulerer underleverandørenes forvaltning av personopplysninger i forbindelse med denne avtalen.

I avtaler mellom databehandler og underleverandører skal underleverandørene pålegges å ivareta alle plikter som databehandleren selv er underlagt i henhold til denne avtalen og lovverket. Databehandler plikter å forelegge avtalene for behandlingsansvarlig på forespørsel.

Databehandler skal kontrollere at underleverandører overholder sine avtalemessige plikter, spesielt at informasjonssikkerheten er tilfredsstillende og at ansatte hos underleverandører er kjent med sine forpliktelser og oppfyller disse.

Behandlingsansvarlig godkjenner at databehandler engasjerer følgende underleverandører for å oppfylle denne avtalen: se **Bilag 3.**

Databehandler kan ikke engasjere andre underleverandører enn de som er nevnt ovenfor uten at dette på forhånd er skriftlig godkjent av behandlingsansvarlig.

Databehandler er ansvarlig for underleverandørens handlinger og unnlatelser som om de var databehandlerens egne.

I tilfeller der den behandlingsansvarlige har godkjent bruk av en underleverandør i henhold til **Bilag 3,** skal databehandleren påse at underleverandøren etterlever eventuelle krav til undertegning av EUs standardavtale og tilleggstiltak i henhold til denne databehandleravtalens punkt 12.

Databehandler plikter å ikke ta i bruk underleverandører før vilkårene i dette punkt 10 og punkt 12 er oppfylt.

11. Behandlingsplaner

Både Databehandler og underleverandører av Databehandler plikter å utarbeide og følge eget prosedyreverk/behandlingsplan som sikrer at deres behandling av personopplysninger utføres i henhold til deres respektive inngåtte databehandleravtale.

Slikt prosedyreverk/behandlingsplan skal fremlegges for Behandlingsansvarlig for dennes kvalitetssikring og godkjenning før behandlingen kan iverksettes.

12. Overføring til land i/og utenfor EU/EØS

Innenfor EU/EØS

Personopplysninger som databehandler forvalter i henhold til denne avtalen, vil bli overført til følgende mottakerland innenfor EU/EØS: **se bilag 3.**

Utenfor EU/EØS

For å overholde kravene i personopplysningslovgivningen for overføring av personopplysninger til databehandler/underleverandører hvor behandlingen utføres utenfor EU/EØS, skal databehandler sørge for at det ikke overføres personopplysninger til land utenfor EØS-området uten overføringsgrunnlag i henhold til personopplysningslovgivningen og dokumentasjon som påviser at vilkårene for å benytte overføringsgrunnlaget er oppfylt.

Overføringer må også oppfylle tilleggskravene fastsatt av EU-domstolen i (EU) C-311/18 (**Schrems II-dommen**). Databehandleren skal i et slikt tilfelle dokumentere dette i **bilag 3**. Identifisering og implementering av tilleggstiltak skal skje for databehandlerens regning.

Personopplysninger som databehandler forvalter i henhold til denne avtalen, vil bli overført til følgende mottakerland utenfor EU/EØS: **se bilag 3**.

Det rettslige grunnlaget for overføring av personopplysninger til de nevnte mottakerland utenfor EU/EØS er: **se bilag 3.**

13. Sikkerhetsrevisjoner og konsekvensutredninger

Databehandler skal jevnlig gjennomføre sikkerhetsrevisjoner av eget arbeid med sikring av personopplysninger mot uautorisert eller ulovlig tilgang, endring, sletting, skade, tap eller utilgjengelighet.

Sikkerhetsrevisjoner skal omfatte databehandlers sikkerhetsmål og sikkerhetsstrategi, sikkerhetsorganisering, retningslinjer og rutiner for sikkerhetsarbeidet, etablerte tekniske, fysiske og organisatoriske sikringstiltak og arbeidet med informasjonssikkerhet hos underleverandører til denne avtalen. Det skal i tillegg omfatte rutiner for varsling av behandlingsansvarlig ved sikkerhetsbrudd og rutiner for testing av beredskaps- og kontinuitetsplaner.

Databehandler skal dokumentere sikkerhetsrevisjonene. Behandlingsansvarlig skal gis tilgang til revisjonsrapportene på forespørsel.

Dersom en uavhengig tredjepart gjennomfører sikkerhetsrevisjoner hos databehandler, skal behandlingsansvarlig informeres om hvilken revisor som benyttes og få tilgang til oppsummeringer av revisjonsrapportene på forespørsel.

14. Plikter ved opphør/oppsigelse

Ved opphør av Avtalen plikter Databehandleren, etter Behandlingsansvarliges valg, å tilbakelevere eller å slette alle personopplysninger som er mottatt på vegne av den Behandlingsansvarlige og som omfattes av denne Avtalen. Ved tilbakelevering skal personopplysningene og andre data overleveres i et standardisert format og medium sammen med nødvendige instruksjoner som muliggjør Behandlingsansvarliges videre bruk av dataene.

Databehandler plikter å slette eller forsvarlig destruere alle dokumenter, data, lagringsmedier mv., som inneholder (kopier av) opplysninger eller data som omfattes av Avtalen og som Databehandleren ikke skal tilbakelevere, eller med hjemmel i annen lov er pålagt å oppbevare. Dette gjelder også for eventuelle sikkerhetskopier.

Databehandleren skal fremlegge skriftlig dokumentasjon på at tilbakelevering eller sletting har funnet sted, i henhold til Behandlingsansvarliges instruksjoner.

15. Mislighold

Ved mislighold av vilkårene i denne databehandleravtalen som skyldes feil eller forsømmelser fra databehandlers side, kan behandlingsansvarlig si opp avtalen med øyeblikkelig virkning. Slikt mislighold vil utgjøre et vesentlig mislighold av Avtalen. Databehandler vil fortsatt være pliktig til å tilbakelevere og slette personopplysninger som forvaltes på vegne av behandlingsansvarlig i henhold til bestemmelsene i punkt 14 ovenfor.

16. Avtalens varighet

Denne databehandleravtalen gjelder frem til opphør av Avtalen.

17. Kontaktpersoner

Kontaktperson hos databehandler for spørsmål knyttet til denne avtalen er: Ingar Hagen, CPO, gdpr@tappin.no

Kontaktperson hos behandlingsansvarlig for spørsmål knyttet til denne avtalen er: {{kontaktnavn}}, {{kontaktemail}}, {{telefon}}.

Brudd på personopplysningssikkerheten skal meldes til behandlingsansvarliges personvernombud.

18. Lovvalg og verneting

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

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

Oslo {{dato}}

På vegne av behandlingsansvarlig	På vegne av databehandler
Navn: {{kontaktnavn}}	Navn: Ingar Hagen
.....	.....
(underskrift)	(underskrift)

BILAG 1 REGISTRERTE OG KATEGORIER AV OPPLYSNINGER

Registrerte

- Deltakere på arrangementer

· ansatte, innleide, brukere, deltakere, besøkende, nettstedets besøkende, leverandører, foredragsholdere.

Kategorier opplysninger

- Navn*
- Telefonnummer*
- E-post adresse*
- Adresse
- Opplysninger om arbeidsgiver
- Tittel/ stilling
- Bilder og personlige videoer
- Samtaler mellom deltakere
- Fødsels- og personnummer
- Kjønn
- Personlige notater
- Statistikk og logger om bruk av systemet*
- Logger over tilsendte e-post og SMS*
- Publiserte meldinger på timeline eller annet sted i systemet*

*Disse kategoriene er alltid registrert, de andre kategoriene er valgfritt basert på behandlingsansvarlig sitt valg.

Særlige kategorier opplysninger

- I enkelte tilfeller lagres det helseopplysninger slik som allergier og funksjonshemminger.

Ytterligere opplysninger

- IP-adresse
- Cookies for bedring av brukeropplevelse
- Dato og tid på kommunikasjon mellom brukere
- Tidspunkt for inn og utlogging
- Geodata → begrenset til land
- Data om adgangskontroll i de tilfeller dette blir levert av Tappin AS → tidspunkt, sesjon.

BILAG 2 INFORMASJONSSIKKERHET

- Sikkerhetsmal https://tinyurl.com/ygajz326
- Avviksskjema https://tinyurl.com/ydn8nxlz
- Sikkerhetsinstruks sikkerhetsansvarlig https://tinyurl.com/yehlwwsq
- Sikkerhetsorganisasjon https://tinyurl.com/yfjcxo3y

BILAG 3 OVERFØRING TIL LAND UTENFOR EØS-OMRÅDET OG UNDERLEVERANDØRER (UNDERDATABEHANDLERE)

1. Overføring til databehandler, land:

Tappin AS, Norge

2. Overføring til underleverandører (underdatabehandler), navn og land:

Databehandler vil benytte seg av følgende underleverandører:

Navn	**Behandlingsaktivitet**	**Sted**
Amazon AWS *	Lagring av data	Dublin, Irland
MongoDB*	Database	Europa
Flowplayer	Video tjenester	Stockholm, Sverige
Whereby	Videomøte tjenester	Norge
Cloudflare *	CDN	Globalt
Google *	Interne verktøy (Google Cloud - e-post, tekstbehandling, regneark, presentasjoner, lagring av filer og dokumenter for interne prosesser)	Europa

* underleverandører som alltid benyttes, de øvrige er frivillige og basert på behandlingsansvarliges ønske(r)

3. Overføringsgrunnlag:

Databehandler/underleverandør skal ikke overføre personopplysninger ut av EØS, eller gi underleverandører utenfor EØS tilgang til personopplysninger, uten etter skriftlig samtykke fra behandlingsansvarlig.

Ved samtykke til overføring av personopplysninger til et land utenfor EØS-området, som ikke er ansett å sikre forsvarlig behandling i henhold til GDPR Artikkel 45, plikter databehandler å inngå avtale på grunnlag av EUs standardavtaler for overføring til databehandlere i tredjeland ((EU) 2021/914) eller annen slik standardavtale som eventuelt har avløst denne.

I disse tilfellene skal databehandler forplikte seg til å påse at tilgang til eller behandling av personopplysninger ikke skjer før:

(i) EUs standardavtaler er undertegnet av den EØS-baserte databehandleren som data eksportør og den ikke EØS-baserte databehandler eller underleverandør som data importør, og

(ii) Databehandler har mottatt den behandlingsansvarliges utvetydige bekreftelse på at eventuelle krav om å gi melding eller innhente godkjenning fra datatilsynsmyndighetene før overføringen anses å være ivaretatt.

4. Mer informasjon om underleverandører

AWS

- AWS Risk Assessment by Tappin

Cloudflare

- Cloudflare Risk Assessment by Tappin

Whereby

- Whereby Risk Assessment by Tappin

Google

- Google Risk Assessment by Tappin

Flowplayer

- Flowplayer Risk Assessment by Tappin

Mongo DB

- MongoDB Risk Assesment by Tappin