Vedlegg 1

Avtale

om databehandling

Mellom

Bits AS, org. nr. 916960190 («**Databehandler»**)

og

Finansinstitusjon, org. nr.xxxxxx («**Behandlingansvarlig»**)

Dato: Se elektronisk signatur	Dato: Se elektronisk signatur
Se elektronisk signatur	Se elektronisk signatur
Bits AS	Finansforetak
Fornavn Etternavn	Fornavn Etternavn

Avtalen er utstedt i et elektronisk eksemplar, hvor partene har mottatt hvert sitt.

1. AVTALENS FORMÅL

Databehandleren vil yte behandlingansvarlig tjenester i forbindelse med at Finansforetaket får tilgang til kundeforholdsregisteret (KFR). Tjenesten reguleres i «KFR-Avtale om tilgang til Kunderegister» (heretter «KFR-avtalen»).

Denne avtalen ("databehandleravtalen") regulerer hvordan personopplysningene skal behandles. Databehandleravtalen skal sikre at personopplysningene behandles i samsvar med kravene i

- Lov og forskrifter om behandling av personopplysninger – som er gjeldende til enhver tid
- EUs personvernforordning (EU 2016/679 GDPR) (samlet benevnt som «personvernregelverket»).

Ved eventuell motstrid mellom vilkår eller avtaler inngått mellom partene i DSOP-prosjekt og databehandleravtalen, hva gjelder behandling av personopplysninger, skal databehandleravtalen ha forrang.

Behandlingansvarlig kan kreve gjennomført endringer i databehandleravtalen, som er nødvendig for å etterleve forpliktelser etter personvernregelverket, ved behov.

1. HVILKE OPPLYSNINGER SOM BEHANDLES OG HVA OPPDRAGET GÅR UT PÅ

Behandlingansvarlig gir databehandler fullmakt til å behandle personopplysninger i forbindelse med databehandlers tjenester, i henhold til KFR-avtalen

Kategorier av type personopplysninger som behandles og hvordan, er beskrevet i **bilag 1** i

«*Bilag databehandleravtale KFR*».

2. DATABEHANDLERS PLIKTER

Databehandler skal følge det til enhver tid gjeldende Regelverket, samt de dokumenterte instrukser for behandling av personopplysninger som behandlingsansvarlig har bestemt skal gjelde gjennom denne Databehandleravtale. Behandlingsansvarlig kan gi ytterligere instruksjoner til Databehandler. Databehandler skal ikke behandle personopplysningene på annen måte enn det som er nødvendig for å levere tjenestene i KFR.

Databehandler skal yte rimelig bistand til behandlingansvarlig, for å sikre at behandlingansvarlig oppfyller kravene i personvernregelverket. Databehandler skal umiddelbart varsle behandlingansvarlig dersom databehandler mener behandlingsansvarliges instrukser er i strid med personvernregelverket.

Databehandler skal, uten unødig opphold, besvare henvendelser fra behandlingansvarlig om behandlingen av personopplysningene. Databehandler plikter videre å bistå behandlingansvarlig med tilgang til personopplysningene ved behov. Henvendelser til databehandleren fra andre som gjelder databehandleravtalen, skal databehandleren videreformidle til behandlingsansvarlig så raskt som mulig. Herunder eventuelle henvendelser fra registrerte vedrørende innsyn, retting, sletting og øvrige rettigheter.

Databehandler plikter å sikre personopplysningers integritet, tilgjengelighet og konfidensialitet, blant annet ved at personopplysninger holdes logisk adskilt fra egne og andres opplysninger og tjenester.

Databehandler skal ha oversikt over hvilke av sine ansatte og eventuelle oppdragstagere som gis tilgang til informasjonssystemet eller til områder og utstyr som inneholder personopplysninger. Tilganger skal begrenses til ansatte som har tjenstlig behov for informasjonen. Enhver bruk av informasjonssystemet skal loggføres.

Databehandleren plikter å påse at samtlige personer som har tilgang til personopplysningene, er kjent med personvernregelverket og forpliktelsene som følger av databehandleravtalen, jf. også punkt 8 nedenfor.

3. BRUK AV UNDERLEVERANDØR

Databehandler skal varsle behandlingansvarlig skriftlig om eventuelle planlagte endringer av underleverandører, eller bruk av nye. senest 30 dager før endringen trer i kraft.

Behandlingsansvarlig kan innen fristen nekte å godkjenne ny underleverandør dersom det foreligger saklig grunn.

Databehandler kan bare overføre personopplysninger og annen taushetsbelagt informasjon til underleverandører og tredjeparter i den utstrekning dette er nødvendig for gjennomføring av KFR-avtalen eller lovbestemte pålegg.

Databehandler skal påse, og er ansvarlig for, at eventuelle underleverandører er kjent med og oppfyller de samme forpliktelser som påligger databehandler etter databehandleravtalen og personvernregelverket. Bruk av underleverandør forutsetter skriftlig avtale mellom databehandler og underleverandør, samt tilfredsstillende dokumentasjon for at kravet til sikkerhet etter punkt 5 er oppfylt.

Databehandler er fullt ansvarlig for underleverandørens utførelse av tjenestene og pliktene etter databehandleravtalen, på samme måte som om databehandleren selv stod for utførelsen.

Databehandler skal føre oversikt over underleverandører som benyttes etter databehandleravtalen, og hvilke oppgaver disse utfører. Oversikten er inntatt i **bilag 2** i «*Bilag databehandleravtale KFR*».

4. SIKKERHET

Databehandleren skal oppfylle de krav til sikkerhet som stilles etter personvernregelverket. Databehandler skal herunder ha etablert en sikkerhetsstrategi, som omfatter organisatoriske og tekniske sikkerhetstiltak. Sikkerhetstiltakene skal ivareta kravene til konfidensialitet, integritet og tilgjengelighet, og stå i forhold til den risikoen som behandlingen av personopplysningene representerer.

Databehandler skal på forespørsel fra behandlingansvarlig fremvise dokumentasjon på sikkerhetsstrategien og sikkerhetstiltakene. Dokumentasjonen skal omfatte sikkerhetstiltak i datasystemene, rutiner for bruk av informasjonssystemet og annen informasjon av vesentlig betydning for informasjonssikkerheten (ansvar, opplæring av ansatte, fysisk sikkerhet mv).

All forsendelse av personopplysninger mellom partene skal, enten det skjer i form av datafiler eller på annen måte, være tilstrekkelig sikret mot innsyn fra uvedkommende. Det samme gjelder avtalt forsendelse eller tilgjengeliggjøring for tredjepart.

Databehandler skal gi nødvendig opplæring til alt personell med tilgang til personopplysningene eller informasjonssystemet, om personvern og sikkerhet og de sikkerhetskravene som følger av denne avtalen.

5. AVVIK

Brudd på personopplysningssikkerheten og andre sikkerhetsbrudd, skal behandles som avvik. Det omfatter bruk av personopplysningene eller informasjonssystemet som er i strid med etablerte rutiner, databehandleravtalen og personvernregelverket.

Databehandler skal ha på plass rutiner og systematiske prosesser for å følge opp avvik. Det skal omfatte gjenoppretting av normalsituasjonen, fjerne årsaken til avviket og å hindre gjentakelse.

Dersom avvik blir oppdaget, eller dersom det er grunn til å tro at det foreligger avvik, skal databehandler umiddelbart, og senest innen 24 timer, rapportere om avviket til behandlingansvarlig.

Meldingen skal inneholde den informasjonen som er påkrevd etter personvernlovgivningen, slik at behandlingansvarlig kan iverksette hensiktsmessige tekniske og organisatoriske tiltak som står i forhold til den oppstått risko, og slik at behandlingsansvarlig enkelt kan sende melding videre til Datatilsynet og eventuelt de registrerte. Databehandler skal yte rimelig bistand slik at behandlingansvarlig kan oppfylle sine forpliktelser til å gi utfyllende informasjon til Datatilsynet og de registrerte, og å svare på spørsmål.

6. SIKKERHETSREVISJONER OG KONTROLL

Databehandler skal gjennomføre sikkerhetsrevisjoner årlig. Revisjonen skal omfatte gjennomgang av sikkerhetsstrategi og rutiner og andre egnede kontrolltiltak. Revisjonen skal dokumenteres. Behandlingansvarlig kan kreve innsyn i dokumentasjonen.

Behandlingansvarlig kan videre kreve skriftlig bekreftelse på databehandlers etterlevelse av personvernregelverket og denne avtalen. Databehandler dekker selv egne kostnader som er forbundet med utøvelse av slik revisjon.

I tillegg kan behandlingansvarlig, eller tredjepart oppnevnt av behandlingansvarlig, gjennomføre kontroll og innsyn i systemer, datadrift, kontroll- og sikkerhetstiltak som er omfattet av databehandleravtalen, for å sikre at den etterleves.

Tilsvarende rett til kontroll og innsyn gjelder for Datatilsynet eller annet relevant tilsynsorgan med hjemmel til innsyn i behandlingsansvarliges virksomhet. Innsyns – og kontrollretten omfatter mulighet for stedlig tilsyn. Databehandler er også forpliktet til å svare på direkte spørsmål og å utlevere dokumentasjon.

7. TAUSHETSPLIKT

Databehandler har taushetsplikt om dokumentasjon og personopplysninger som vedkommende får tilgang til i henhold til et vilkår eller avtale inngått mellom partene og

databehandleravtalen. Det gjelder også øvrig informasjon som databehandler blir kjent med i forbindelse med gjennomføringen av KFR-avtalen. Det innebærer at personopplysningene og øvrig informasjon skal behandles konfidensielt, og ikke utleveres eller gjøres tilgjengelig for utenforstående, uten grunnlag i denne avtalen eller eksplisitt pålegg fra behandlingansvarlig. Ved eventuelt pålegg om utlevering fra offentlig myndighet, skal databehandler varsle behandlingansvarlig.

Taushetsplikten gjelder databehandlers ansatte, herunder konsulenter og andre som er engasjert av virksomheten, og underleverandører som handler på databehandlers vegne i forbindelse med gjennomføring av KFR-avtalen og databehandleravtalen. Alt personell som behandler personopplysninger eller annen taushetsbelagt informasjon, skal avgi taushetserklæring og gjøres kjent med hva taushetsplikten innebærer.

Behandlingansvarlig skal beskytte fortrolig sikkerhets-, forretnings- og/eller kundeinformasjon som behandlingansvarlig mottar fra databehandler og underleverandører, eller som behandlingansvarlig blir kjent med i forbindelse med gjennomføring KFR-avtalen.

Behandlingansvarlig skal ikke uberettiget utnytte, dele eller videreformidle slik taushetsbelagt informasjon.

Taushetsplikten gjelder også etter at denne avtalen er opphørt. Ansatte eller andre som fratrer sin tjeneste, skal pålegges taushetsplikt også etter fratredelsen.

8. OVERFØRING TIL UTLANDET

Databehandler skal ikke overføre personopplysninger ut av EU/EØS uten skriftlig godkjennelse fra behandlingansvarlig. Hvis slik overføring skal skje må det inngås avtale om overføringsgrunnlag, for eksempel model clauses, binding corporate rules eller privacy shield.

9. ANSVAR/MISLIGHOLD

Databehandlers ansvar er begrenset til direkte tap som følger av feil oppstått i forbindelse med databehandlers plikter etter databehandleravtalen og KFR-avtalen. Indirekte tap omfattes ikke.

10. AVTALENS VARIGHET, PÅLEGG OM STANS, OPPSIGELSE MV

Avtalen gjelder så lenge databehandleren behandler eller har tilgang til personopplysninger på vegne av behandlingansvarlig i henhold til KFR-avtalen.

Ved brudd på databehandleravtalen eller personvernregelverket, kan behandlingansvarlig pålegge databehandleren å stoppe den videre behandlingen av opplysningene med øyeblikkelig virkning.

11. PLIKTER VED OPPHØR/OPPSIGELSE

Ved opphør av databehandleravtalen plikter databehandleren, etter behandlingsansvarliges valg, å tilbakelevere eller slette alle personopplysninger som er mottatt på vegne av den behandlingsansvarlige og som omfattes av databehandleravtalen. Ved tilbakelevering skal

personopplysningene og andre data overleveres i et standardisert format og medium sammen med nødvendige instruksjoner som muliggjør behandlingsansvarliges videre bruk av data.

Databehandler plikter å slette eller forsvarlig destruere alle dokumenter, data, lagringsmedier mv., som inneholder (kopier av) opplysninger eller data som omfattes av databehandleravtalen 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.

Behandlingsansvarliges rett til revisjon etter pkt. 7, for å sikre at databehandlers plikter er oppfylt, gjelder også etter opphør av databehandleravtalen, for så vidt gjelder behandlingen av personopplysninger.

12. ØVRIGE PLIKTER OG RETTIGHETER

Øvrige plikter og rettigheter følger av KFR-avtalen. De samme kontaktpersoner gjelder for databehandleravtalen som for KFR-avtalen. Ved eventuell overdragelse KFR-avtalen til andre parter, skal databehandleravtalen overdras samtidig.

13. LOVVALG OG VERNETING

Databehandleravtalen er underlagt norsk rett. Oslo tingrett vedtas som rette verneting.