

Databehandleravtale

Bakgrunn for Databehandleravtalen

1. Denne databehandleravtalen beskriver rettigheter og forpliktelser som gjelder når databehandleren behandler personopplysninger på vegne av behandlingsansvarlige. Herunder:

- Når databehandler er Uni Micro AS, eller dennes representanter
- Når databehandler er Regnskapsbyrå, eller dennes representanter
- Når Uni Micro AS, eller dennes representanter er underleverandører (Til Regnsk.byrå)

Uni Micro AS leverer en én-til-mange-tjeneste og inngår ikke individuelle databehandleravtaler med hver enkelt kunde. Denne databehandleravtalen gjelder derfor for alle programsuiter Uni Micro AS leverer, og alle brukerne som benytter tjenesten.

2. Avtalen er utformet for at partene skal overholde personopplysningsloven, samt artikkel 28 nr. 2. 3 Europaparlaments- og rådsforordning (EF) 2016/679 av 27 april 2016 om beskyttelse av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger og om oppheving av direktiv 95/46 / EF (Data Protection Regulation) som fastsetter spesifikke krav til innholdet i en databehandleravtale.

3. Databehandler leverer programvareløsninger for økonomi, logistikk, regnskap og lønn (ERP), til det norske/europeiske markedet. Den Behandlingsansvarlige (kunde) bestemmer formålet med behandlingen av personopplysningene og hvilke midler som skal benyttes. Databehandleren har forpliktet seg til å levere tjenestene beskrevet i ordinær Bruksretts- og Vedlikeholdsavtale/EULA ("Hovedavtalen"). Databehandleravtalen inngår som bilag til denne «Hovedavtalen».

Databehandlerens behandling av personopplysninger er gjort for å oppfylle partenes "hovedavtale". Databehandleravtalen og "hovedavtalen" er gjensidig avhengige og kan ikke termineres separat. Databehandlingsavtalen kan imidlertid - uten å si opp hovedavtalen - bli erstattet av en annen gyldig databehandlingsavtale.

4. Denne databehandleravtalen har forrang i forhold til lignende bestemmelser i andre avtaler mellom partene, herunder "hovedavtalen".

5. For denne avtalen er det vedlagt fire vedlegg. Vedleggene er en integrert del av databehandleravtalen.

6. Databehandleravtalens **vedlegg A** inneholder detaljer om behandlingen, inkludert formål og art av behandlingen, typen av personopplysninger, kategorier av registrert og varighet av behandlingen.

7. Databehandleravtalens **vedlegg B** inneholder den behandlingsansvarliges betingelser for, at databehandleren kan gjøre bruk av eventuelle underleverandører, så vel som en liste over eventuelle underleverandører som er godkjent av den behandlingsansvarlige.

8. Databehandleravtalens **Vedlegg C** gir mer detaljerte instruksjoner om hvilken behandling databehandleren skal utføre på vegne av den behandlingsansvarlige hvilke sikkerhetforanstaltninger (avhengig av behandlingen) som minst må finnes, og hvordan det eventuelt skal føres tilsyn med

databehandleren og eventuelle underleverandører.

9. **Vedlegg D** til databehandleravtalen inneholder partenes mulige regulering av saker som ikke er angitt i databehandleravtalen eller partenes "hovedavtale", herunder vederlag for bistand o.l.

10. Databehandleravtalen og tilhørende vedlegg skal oppbevares skriftlig, herunder elektronisk.

11. Denne databehandleravtale fritar ikke databehandleren for forpliktelser som etter personopplysningsloven eller enhver annen lovgivning er direkte er pålagt databehandleren.

Definisjoner:

For å få best mulig utbytte av informasjonen som gis, vil vi gi en oversikt over noen sentrale begreper som benyttes i forbindelse med personvernlovgivningen / GDPR:

«**Personopplysninger**»: Enhver opplysning om en identifisert eller identifiserbar fysisk person.

«**Behandling**»: Enhver operasjon eller rekke av operasjoner som gjøres med personopplysninger, f.eks. innsamling, registrering, organisering, strukturering, lagring, tilpasning eller endring, gjenfinning, konsultering, bruk, utlevering ved overføring, spredning eller alle andre former for tilgjengeliggjøring, sammenstilling eller samkjøring, begrensning, sletting eller tilintetgjøring.

«**Registrert**»: En fysisk person hvis personopplysninger behandles. Dette kan være en kunde, ansatt, kontaktperson e.l.

«**Behandlingsansvarlig**»: en 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. (Kunde/Klient i våre systemer).

«**Databehandler**»: En fysisk eller juridisk person, offentlig myndighet, institusjon eller ethvert annet organ som behandler personopplysninger på vegne av den behandlingsansvarlige.

Uni Micro vil være databehandler ovenfor kunder/klienter som har et kundeforhold til Uni Micro. Regnskapsbyråer vil være databehandler ovenfor kunder/klienter som har et kundeforhold til byrået, (oppdragsavtale) I dette tilfellet vil Uni Micro være en underleverandør til byrået.

«**Behandlingsgrunnlag**»: En grunnleggende forutsetning for at behandling av personopplysninger skal være lovlig, er at den bygger på et gyldig behandlingsgrunnlag. Dette kan etter personvernforordningen artikkel 6 være blant annet ulike nødvendighetsgrunner, herunder at behandlingen er nødvendig for å overholde lover og regler, gjennomføre en avtale den registrerte er part i, eller at behandlingen er nødvendig for formål knyttet til de berettigede interessene som forfølges av den behandlingsansvarlige eller en tredjepart.

Det er den behandlingsansvarlige selv som må vurdere om den har behandlingsgrunnlag i hvert enkelt tilfelle, f.eks. om man omfattes av lover og regler som gjør det nødvendig å behandle personopplysninger.

Er du bokføringspliktig, vil behandlingsgrunnlaget m.a. være overholdelse av «Lov om bokføring».

Den behandlingsansvarliges rettigheter og plikter:

1. Den behandlingsansvarlige har overfor omverdenen (herunder den registrerte) ansvar for at behandling av personopplysninger skjer innenfor rammene av personvernforordningen og personopplysningsloven.
2. Den behandlingsansvarlige har derfor både rettighetene og forpliktelsene til å ta avgjørelser om formålene og hvilke midler som er nødvendig for behandling.
3. Den behandlingsansvarlige er ansvarlig for at det er et rettsgrunnlag for behandlingen som databehandleren er pålagt å utføre.

Databehandlerens rettigheter og plikter:

1. Databehandleren kan kun behandle personopplysninger etter instruks fra behandlingsansvarlige, med mindre annet er påkrevd av unionsretten eller den nasjonale lovgivningen i medlemsstatene (EØS) som databehandleren er underlagt. I så fall underretter databehandleren den behandlingsansvarlige om dette kravet før behandling, med mindre loven forbyr slik varslings med henvisning til viktige samfunnsmessige interesser, Ref. Art 28 punkt. 3 (a).
2. Databehandleren skal umiddelbart informere behandlingsansvarlige, hvis en instruksjon for databehandleren er i strid med personvernforordningen, personopplysningsloven eller andre personvernbestemmelser i EU-lovgivning eller nasjonal lovgivning.

Konfidensialitet

1. Databehandleren sikrer at bare de personer som til enhver tid er autorisert til å gjøre det, har tilgang til personopplysningene som behandles på vegne av den behandlingsansvarlige. Tilgang til informasjonen må derfor umiddelbart avsluttes dersom autorisasjonen er fratatt eller utløpt.
2. Kun personer som er autorisert for tilgang til personopplysninger, kan gis nødvendig tilgang for å oppfylle databehandlerens forpliktelser overfor den behandlingsansvarlige.
3. Databehandleren sikrer at de personer som er autorisert til å behandle personopplysninger på vegne av den behandlingsansvarlige har forpliktet seg til konfidensialitet eller er underlagt passende lovbestemt konfidensialitet (Taushetserklæring).
4. Databehandleren skal etter anmodning fra den behandlingsansvarlige, kunne påvise at de ansatte er underlagt nevnte konfidensialitet/taushetsplikt.

Behandlingsikkerhet

1. Databehandleren skal gjennomføre alle tiltak som kreves i artikkel 32 i databeskyttelsesforskriften, Det iverksettes hensiktsmessige tekniske og organisatoriske tiltak for å sikre et godt og tilfredsstillende sikkerhetsnivå.

2. Ovennevnte forpliktelse innebærer at databehandleren kan gjennomføre en risikovurdering og deretter iverksette nødvendige tiltak for å løse identifiserte risikoer. Blant annet kan det, være følgende tiltak:
 - a) Pseudonymisering og kryptering av personopplysninger
 - b) Evne til å sikre fortsatt konfidensialitet, integritet, tilgjengelighet og robusthet i behandlingssystemer og tjenester.
 - c) Evne til rettidig gjenoppretting av tilgjengelighet og tilgang til personlige data i tilfelle fysisk eller teknisk hendelse.
 - d) En prosedyre for periodisk testing, vurdering og evaluering av effektiviteten av tekniske og organisatoriske tiltak for å sikre behandlingssikkerhet.
3. I forbindelse med det ovennevnte må databehandleren iverksette minst sikkerhetsnivået og tiltakene som er angitt i dette tilleggets vedlegg C.
4. Partenes mulige regulering / avtale om godtgjørelse eller lignende i forbindelse med den behandlingsansvarlige eller databehandlerens påfølgende behov for å tilveiebringe ekstra sikkerhet vil fremgå av partenes "hovedavtale" eller i Vedlegg D.

Bruk av underleverandører

1. Databehandleren må overholde betingelsene i artikkel 28 nr. 1 i personvernforordningen. 2 og 4, for å bruke en annen databehandler (underleverandør) .
2. Databehandleren har den behandlingsansvarliges generelle godkjennelse til å bruke andre underleverandører, i tillegg til de som står oppført i **vedlegg B.2** i denne avtalen.
3. Databehandleren må likevel underrette den behandlingsansvarlige ved eventuelle planer om å skifte ut eller bruke nye underleverandører. Den behandlingsansvarlige må motta en slik underretning minimum 3 uker før endringen trer i kraft.
4. Den behandlingsansvarlige skal ha mulighet til å motsette seg endringene, og skal meddele databehandleren om dette senest 1 uke etter underretningen er mottatt. Dersom den behandlingsansvarlige motsetter seg endringene, vil dette medføre opphør av denne avtale, samt «hovedavtalen».
5. Den behandlingsansvarliges vilkår og betingelser for databehandlerens bruk av eventuelle underleverandører finnes i **vedlegg B.1** i denne avtalen. Den behandlingsansvarliges godkjenning av spesifikke underleverandører er oppført i **vedlegg B.2** i denne avtalen.
6. Databehandleren sørger for å pålegge underleverandører de samme forpliktelsene som databehandleren selv har etter denne avtalen, gjennom en kontrakt eller andre juridiske dokumentet under EUs lovgivning eller nasjonal lov - hvor det blir gitt de nødvendige garantier for at underleverandøren vil gjennomføre de nødvendige tekniske og organisasjonsmessige tiltak på en måte som tilfredsstiller kravene i personopplysningsloven.
7. Underleverandøravtalene og eventuelle endringer i disse kan gjøres tilgjengelig for den behandlingsansvarlige - ved den behandlingsansvarliges forespørsel - Eventuelle kommersielle vilkår, for eksempel priser som ikke påvirker databeskyttelsesinnholdet i underleverandøravtalen, skal ikke gjøres tilgjengelig for den behandlingsansvarlige. Nærmere om tilgang/form og innhold er oppført i **Vedlegg B.7** i denne avtalen.
8. Hvis underleverandøren ikke oppfylder sine plikter som omhandlet i denne avtale, står databehandleren fullt ut ansvarlige overfor den behandlingsansvarlige for oppfyllelse av underleverandørens forpliktelser.

Overføring av informasjon til tredjeland eller internasjonale organisasjoner

1. Databehandleren kan kun behandle personopplysninger etter dokumenterte instruksjoner av behandlingsansvarlige, herunder når det gjelder overføring (lagring, formidling og intern bruk) av personopplysninger til tredjeland eller internasjonale organisasjoner med mindre det følger av EUs lovgivning eller nasjonal lovgivning, som databehandleren er gjenstand for; I så fall informerer databehandleren den behandlingsansvarlige om dette lovlige kravet før behandling, med mindre gjeldende regelverk foryr slik informasjon av hensyn til viktige samfunnsmessige interesser, jf. art 28, stk. 3 litra a.
2. Uten den behandlingsansvarliges instruksjon eller godkjenning kan databehandleren - innenfor rammen av databehandlingsavtalen - blant annet ikke:
 - a) overføre personopplysninger til en underleverandør i et tredjeland eller i en internasjonal organisasjon,
 - b) overlate behandling av personopplysninger til en underleverandør i et tredjeland,
 - c) behandle personopplysninger i en annen av underleverandørens avdelinger i et tredjeland.
3. Den behandlingsansvarliges mulige instruksjon eller godkjenning av overføring av personopplysninger til et tredjeland vil fremgå av vedlegg C.5 i denne avtalen

Bistand til den behandlingsansvarlige

1. Databehandleren bistår, under hensyntagen til behandlingens karakter, så langt som mulig den behandlingsansvarlige ved hjelp av hensiktsmessige tekniske og organisatoriske tiltak, med oppfyllelsen av den behandlingsansvarliges plikt til å svare på forespørsler for å utøve de registrertes rettigheter som definert i forordningens kapittel 3. Dette betyr at Databehandleren så langt som mulig skal bistå behandlingsansvarlig for at den behandlingsansvarlige sikrer samsvar med:
 - a) Opplysningsplikten for innsamling av personopplysninger hos den registrerte
 - b) Opplysningsplikten, hvis personopplysninger ikke er innsamlet hos den registrerte.
 - c) Den registrertes innsynsrett.
 - d) Retten til utbedring/korreksjoner
 - e) Retten til å slette ("retten til å bli glemt")
 - f) Retten til begrensning av behandling.
 - g) Varslingsforpliktelse i forbindelse med utbedring eller sletting av personopplysninger eller begrensning av behandling.
 - h) Retten til dataportabilitet.
 - i) Retten til innsigelse
 - j) Retten til å motsette seg resultatet av automatiske individuelle beslutninger, inkludert profiling

2. Databehandleren bistår den behandlingsansvarlige med å sikre etterlevelse av behandlingsansvarliges plikter under dataforordningens artikkel 32-36 under hensyntagen til behandlingens karakter og den informasjonen som er tilgjengelig for databehandleren, se. Art 28 punkt. 3,
Dette innebærer at databehandleren under hensyntagen til behandlingens karakter skal bistå den behandlingsansvarlige til å sikre overholdelse av:
 - a) Forpliktelsen til å iverksette hensiktsmessige tekniske og organisatoriske tiltak for å sikre et nivå av sikkerhet som samsvarer med å dekke den risiko som er forbundet med behandlingen
 - b) Plikten til å varsle brudd på persondatasikkerheten til tilsynsmyndigheten (Datatilsynet) uten ugrunnet opphold, og om mulig innen 72 timer, etter at den behandlingsansvarlige har blitt klar over misligholdet, med mindre det er usannsynlig at det innebærer en risiko for individers rettigheter og friheter.
 - c) Plikten til - uten ugrunnet opphold - å informere den/de registrerte om brudd på persondatasikkerheten hvis et slikt brudd er sannsynlig å utgjøre en høy risiko for individers rettigheter og friheter
 - d) Plikten til å gjennomføre en konsekvensanalyse vedrørende datasikkerhet, dersom en type behandling trolig vil innebære en stor risiko for individers rettigheter og friheter
 - e) Plikten til å konsultere tilsynsmyndigheten (Datatilsynet) før behandling, der en konsekvensanalyse viser at behandling vil føre til en høy risiko i fravær av tiltak gjennomført av databehandleren for å begrense risikoen.
3. Databehandleren (Uni Micro AS) vil kunne ta betalt for tjenester som gjelder bistand beskrevet ovenfor til den behandlingsansvarlige. Partenes eventuelle regulering / avtale for betaling eller lignende med hensyn til databehandlerens bistand til den behandlingsansvarlige etter denne avtalen - vil fremkomme på partenes "Hovedavtale" og/eller i denne avtalens **vedlegg D**. Eventuelle prisendringer og andre endringer/presiseringer som gjelder hva/hvilke tjenester eller funksjoner/verktøy som til enhver tid er omfattet av betaling, vil bli varslet minimum 1 mnd. før de innføres, og bli lagt fortløpende til **vedlegg D** i denne avtale.

Melding om brudd på persondatasikkerheten

1. Databehandleren skal uten opphold informere den behandlingsansvarlige eller dens representant, etter å ha vært klar over at det har vært brudd på persondatasikkerheten hos databehandleren eller en eventuell underleverandør.
Databehandlerens varsel til den behandlingsansvarlige skal, hvis mulig, skje senest 24 timer etter at databehandler ble klar over bruddet, slik at behandlingsansvarlige har mulighet til å etterleve sin mulig plikt til å melde fra til bruddet til tilsynsmyndigheten innen 72 timer.
2. I samsvar med denne avtalens punkt b (nedenfor), skal databehandleren - under hensyntagen til behandlingens natur, og tilgjengelig informasjonen - bistå den behandlingsansvarlige til å gi melding om brudd på persondatasikkerheten til tilsynsmyndigheten. Dette kan bety at databehandleren bl.a. skal bistå med å gi følgende opplysninger, slik det er fastsatt i artikkel 33 nr. 3 i personvernforordningen.

- a) Naturen av bruddet på persondatasikkerheten, herunder om mulig kategoriene og omtrentlig antall berørte registrerte samt kategoriene og omtrentlig antall berørte registreringer av personopplysninger.
- b) Sannsynlige konsekvenser av brudd på personopplysninger.
- c) Tiltakene som er truffet eller foreslås truffet for å håndtere bruddet på persondatasikkerheten, herunder om det er hensiktsmessig, tiltak for å begrense mulig skadevirkninger

Sletting og tilbakelevering av data

1. Ved opphør av tjenester knyttet til behandling som kreves, forpliktes databehandleren til, etter den behandlingsansvarliges valg, å slette eller returnere alle personlige data til den behandlingsansvarlige, samt å slette eksisterende egne kopier, med mindre EU lov eller nasjonal lov foreskriver lagring av personopplysningene. Databehandleren velger selv hvilket format slike data blir overlevert på, men det må være innenfor det som kan betegnes som et standard-format, f.eks. excel, eller lignende. Dersom databehandleren gjør tilgjengelig verktøy/funksjonalitet hvor den behandlingsansvarlige, eller dennes representant selv kan hente og slette (herunder anonymisere/scramble) data, anses dette som oppfyllelse av databehandlerens forpliktelse på dette punkt, og den behandlingsansvarlige vil selv være ansvarlig for at sletting og tilbakelevering finner sted. Databehandler vil i dette tilfellet kun være ansvarlig for å slette egne ekstra kopier av datasett, og dokumentere dette.

Tilsyn og revision

1. Databehandler gir behandlingsansvarlig all nødvendig informasjon for å påvise databehandlerens etterlevelse av personvernforordningens artikkel 28 og denne avtalen, og gir mulighet for, og bidrar til, revisjoner (herunder inspeksjoner), utført av behandlingsansvarlig eller en annen revisor som er autorisert av den behandlingsansvarlige.
2. Den detaljerte prosedyren for den behandlingsansvarliges tilsyn av databehandleren fremgår av **Vedlegg C** i denne avtale.
3. Den behandlingsansvarliges tilsyn med eventuelle underleverandører skjer gjennom databehandleren. Detaljene ved slik prosedyre fremgår av **Vedlegg C** i denne avtale.
4. Databehandleren er forpliktet til å gi myndigheter som etter den til enhver tid gjeldende lovgivning har tilgang til den behandlingsansvarliges og databehandlerens fasiliteter, eller representanter som opptrer på myndighetens vegne, tilgang til databehandleren sine fysiske fasiliteter mot riktig identifikasjon.

Partenes avtaler om andre forhold

1. En eventuell (særlig), regulering av konsekvensene av partenes mislighold av databehandleravtalen vil fremgå av partenes "hovedavtale" eller av denne avtalens **Vedlegg D**.
2. En eventuell regulering av andre forhold mellom partene vil fremgå av partenes "hovedavtale" eller av denne avtalens **Vedlegg D**.

Ikrafttredelse og oppsigelse

1. Denne avtalen trer i kraft ved elektronisk aksept av vilkår (databehandleravtale) som blir tilgjengelig ved installasjon/oppdateringer av programvare levert av Uni Micro AS, (som akseptert og inngått i "Hovedavtale").
2. Avtalen kan reforhandles av begge parter dersom loven endres eller uoverensstemmelser i avtalen gir anledning til dette.
3. Partenes eventuelle regulering / avtale om betaling, vilkår, betingelser eller lignende med hensyn til endringer i denne avtale vil fremgå av partene "hovedavtale" eller i denne avtalens **Vedlegg D**.
4. Oppsigelse av databehandleravtalen kan skje i henhold til de oppsigelsesvilkår, inkl. eventuelt oppsigelsesvarsel, som angitt i "hovedavtalen".
5. Avtalen er gjeldende så lenge behandlingen består. Uansett "hovedavtalens" og / eller databehandleravtalens oppsigelse, vil databehandleravtalen gjelde inntil behandlingen avsluttes og fram til sletting av data hos databehandleren og eventuelle underleverandører er foretatt.

Kontaktpersoner / kontaktpunkter til den behandlingsansvarlige og databehandleren

1. Partene kan kontakte hverandre gjennom følgende kontaktpersoner / kontaktpunkter:
 - a) Databehandler: Som angitt i "Hovedavtale" eller til support@unimicro.no – tlf.: 56599100
 - b) Behandlingsansvarlig: Som angitt i "Hovedavtale"
2. Partene må kontinuerlig informere hverandre om endringer vedrørende kontakt / kontaktpunkt som gjelder følgende informasjon: Navn – Adresse – Telefon - E-post

Vedlegg A informasjon om behandling:

Databehandleravtalen gjelder når følgende Produkter/tjenester benyttes:

1) Uni Økonomi V3:

Funksjon	Databehandler/Underlev.	Gjelder for
Online Backup	Uni Micro	Alle data i løsningen
Supportbackup	Uni Micro (Support/Konsulent)	Alle data i løsningen
Fjernoppkobling / Skjermdeling	Uni Micro (Support/Konsulent)	Data som blir delt

Det er kun når Uni Micro mottar backuper for feilsøking, support og konsulenthjelp, eller bistår med support i form av fjernoppkobling mot den behandlingsansvarlige, databehandleravtalen vil gjelde (når Uni Micro behandler data).

2) Uni24 og Uni Economy:

Databehandleravtalen **gjelder alltid**, som følge av at Uni Micro har ansvar for lagring/drift.

Formål:

Formålet med databehandler sin behandling av personopplysninger på vegne av den behandlingsansvarlige er generelt:

Gjennomføre «Hovedavtalen», ved at den behandlingsansvarlige eller dennes representanter kan benytte systemet (programsuite), som eies og forvaltes av Uni Micro AS, og eventuelle tilhørende integrerte systemer – **for å kunne føre regnskap, utstedte faktura og foreta utlønning og rapportering (Mva, A-melding o.l.) i.h.h.t. norsk lov.** (Det vises her spesielt til oppbevaringsplikt for denne type data / Lagring av data).

Behandlingen er ikke tidsbegrenset og varer til avtalen sies opp eller avbrytes av en av partene.

(Alle programsuiter)

Kategorier av personopplysn.	Kategorier av registrerte	Formålet med behandlingen
Personalialia: Navn, fødselsdato/pers.nr., alder, kundenummer, relasjoner, kjønn m.v.	Behandlingsansvarlige sine kunder, leverandører, ansatte	Gjennomføre «Hovedavtalen», herunder konsulenttenester og support knyttet til denne, samt lagring av data (Online Backup, Uni24, Uni Economy)
Kontaktinformasjon: Adresse, e-post, mobil/tlf.nr., land,	Behandlingsansvarlige sine kunder, leverandører, ansatte, kontaktpersoner	Gjennomføre «Hovedavtalen», herunder konsulenttenester og support knyttet til denne, samt lagring av data (Online Backup, Uni24, Uni Economy)
Transaksjonsinformasjon Lønn: Timeføringer, fravær, sykdom, lønn, fagforeningstilhørighet, skatt m.v.	Behandlingsansvarlige sine ansatte	Gjennomføre «Hovedavtalen», herunder konsulenttenester og support knyttet til denne, samt lagring av data (Online Backup, Uni24, Uni Economy)
Transaksjonsinformasjon annet: kredittrating, inkassosaker, purringer, bet.betingelser, kredittgrenser m.v.	Behandlingsansvarlige sine kunder	Gjennomføre «Hovedavtalen», herunder konsulenttenester og support knyttet til denne, samt lagring av data (Online Backup, Uni24, Uni Economy)
Transaksjonsinformasjon teknisk: Påloggingsinformasjon, IP-adresser, loggdata, analysedata o.l.	Behandlingsansvarlige sine ansatte/brukere Databehandler sine ansatte/brukere	Gjennomføre «Hovedavtalen», herunder konsulenttenester og support knyttet til denne, samt lagring, sikring, overvåkning m.m. av data (Online Backup, Uni24, Uni Economy)

Vedlegg B Betingelser for databehandlerens bruk av underleverandører, og oversikt over godkjente underleverandører

B.1 Generell godkjennelse av underleverandører

Databehandleren har den behandlingsansvarliges generelle godkjennelse til å bruke andre underleverandører enn de som fremgår i pkt. B.2 under. Databehandleren må likevel underrette den behandlingsansvarlige ved eventuelle planer om å skifte ut eller bruke nye underleverandører. Den behandlingsansvarlige må motta en slik underretning minimum 3 uker før endringen trer i kraft.

Slik underretning anses utført ved å benytte eksisterende system for generell informasjonsmelding som er tilgjengelig som en del av leveransen i «hovedavtalen», eller ved annen direkte henvendelse.

B.2 Godkjente underleverandører

Den behandlingsansvarlige har når databehandleravtalen / "Hovedavtalen" trer i kraft godkjent bruk av følgende underleverandører:

Uni Economy:

Navn	Org.nr.	Nettadresse	Type behandling
MS-Azure	957 485 030	https://azure.microsoft.com	Drift / Lagring
One Signal		https://onesignal.com	Drift/Overvåkning/Analyse
SendGrid		https://sendgrid.com	Drift/Overvåkning/Analyse
Raygun		https://raygun.com	Drift/Overvåkning/Analyse
Microsoft Vision		https://azure.microsoft.com/en-us/services/cognitive-services/computer-vision/	OCR-skanning (inng.faktura)
Wistia		https://wistia.com	Drift/Overvåkning/Analyse
Iitix,io			Drift/Overvåkning/Analyse
akamaihd.net			Drift/Overvåkning/Analyse
AltInn		https://altinn.no	Skattemelding, A-melding
HubSpot		https://hubspot.com	Lead, CRM-oppfølging
Google		gstatic.com googleapis.com	Drift/Overvåkning/Analyse

Uni 24:

Navn	Org.nr.	Nettadresse	Type behandling
MS-Azure	957 485 030	https://azure.microsoft.com	Drift / Lagring
Elastic E-mail	n/a	https://elasticemail.com	Meldingsformidling (faktura på epost m.a.)

Uni Økonomi V3:

Navn	Org.nr.	Nettadresse	Type behandling
Ingen	-	-	-

Den behandlingsansvarlige **har spesifikt godkjent bruk av ovennevnte underleverandører**, til nettopp den behandling som er beskrevet. Databehandleren kan ikke - uten den behandlingens ansvarliges aksept - benytte den enkelte underleverandør til en annen behandling enn beskrevet, annet enn dersom det er for å understøtte nye produkter (fra eksisterende underleverandør) utover de som er beskrevet.

Samarbeidspartnere

Alle våre programsuiter har mange ulike integrasjoner mot andre 3.parts leverandører/systemer. Det kan være alt fra Remittering, Inkasso, Nettbutikk o.l. som man har egne tilganger til på innsiden av våre programsuiter - til mer direkte (skreddersøm) integrasjoner som man kanskje selv har fått ordnet gjennom en 3.parts leverandør (eller på egen hånd), f.eks. en dataimport/eksport løsning. Felles for alle slike integrasjoner, er at den behandlingsansvarlige selv aktivt må velge å ta dette i bruk.

Det er da en forutsetning at den behandlingsansvarlige har egne avtaler om bruk av slike ulike produkter / integrasjoner direkte med ulike samarbeidspartnere (Ordinær Lisensavtale). En slik avtale kan – og vil normalt, etter at GDPR er trådt i kraft, omfatte en egen databehandleravtale som nærmere spesifiserer vilkårene for behandling av personopplysninger.

Den behandlingsansvarlige må selv sørge for å få Databehandleravtaler (underleverandøravtaler), på plass i.f.h.t. slike integrasjoner med de 3.parter som da evt. vil bli å betrakte som databehandlere.

Under vil vi derfor vise oppstilling av de 3.parter (Samarbeidspartnere), som vi har laget tilganger for på innsiden av våre programsuiter - slik at du som behandlingsansvarlig har en oversikt over hvilke 3.parter du bør få en egen databehandleravtale med.

Uni Økonomi V3:

Navn	Org.nr.	Nettadresse	Type Integrasjon
NETS Branch Norway	996 345 734	https://nets.no	Fakturaprint Autobank (Ocr/Remittering) E-faktura (B2C) Avtalegiro
Uni Micro Web AS	883 427 912	https://unimicro.no	Nettbutikk
Travel Text		https://traveltext.no	Reise og Utlegg
Mobile Worker		https://mobileworker.no	Prosjektadministrasjon
IDFY		https://idfy.no	BankID
Sticos		https://sticos.no	Fagstøtte, oppslag portal
Infotjenester		https://infotjenester.no	Fagstøtte, oppslag portal
Zdata		http://zdata.no	Bankavstemming
Link Mobility		https://linkmobility.no	Kunde/regnsk. opplysninger
Digitroll AS	919 074 604	http://digitroll.no	Nettbutikk
Alt Inn Inkasso			Innkrevning, purring, inkasso
Akros			Innkrevning, purring, inkasso
Aktiv Kapital			Innkrevning, purring, inkasso
Connecto			Innkrevning, purring, inkasso
Credicare			Innkrevning, purring, inkasso
Creno			Innkrevning, purring, inkasso
Kredinor			Innkrevning, purring, inkasso

Kreditorforeningen			Innkreving, purring, inkasso
Lindorff/Bisnode			Innkreving, purring, inkasso
Pacta			Innkreving, purring, inkasso
Totalkapital			Innkreving, purring, inkasso

Uni Economy:

Navn	Nettadresse	Type Integrasjon
Z-Data	https://zdata.no	Autobank, distribusjon bankfiler
TravelText	https://pilot.unieconomy.no/#/marketplace/integrations	Reise og Utlegg
Hokas	https://pilot.unieconomy.no/#/marketplace/integrations	Innkreving, purring, inkasso
OneStopReporting	https://pilot.unieconomy.no/#/marketplace/integrations	Rapporter, oversikter
EasyUpdate	https://easyupdate.no/	Nettbutikk
VIPPS	https://pilot.unieconomy.no/#/marketplace/integrations	Fakturadistribusjon, betalingsløsning

Vedlegg C Instruks vedrørende behandling av personopplysninger

C.1 Behandlingens gjenstand / instruksjon

Databehandlerens behandling av personopplysninger på vegne av den behandlingsansvarlige skjer ved, at databehandleren:

a) Drifter og/eller lagrer data i system som angitt i «Hovedavtalen», og som den behandlingsansvarlige eller dennes representanter kan benytte, og som eies og forvaltes av Uni Micro AS, og eventuelle tilhørende integrerte systemer – for å kunne føre regnskap, utstede faktura og foreta utlønning og rapportering (Mva, A-melding o.l.) i.h.h.t. norsk lov.

b) Gir nødvendig assistanse etter forespørsel fra den behandlingsansvarlige, og/eller videreutvikler og kvalitetssikrer systemet - i form av gjennomgang / analyse av data, feilsøking, opplæring, testing og utbedring til bruk av system nevnt i pkt. a) ovenfor, eller til lokalt installert system (v3) som bestemt i «Hovedavtalen» – for å kunne føre regnskap, utstede faktura og foreta utlønning og rapportering (Mva, A-melding o.l.) i.h.h.t. norsk lov.

C.2 Behandlingssikkerhet

Databehandleren har rett og plikt til å ta avgjørelser om de tekniske og organisatoriske sikkerhetstiltak som kan benyttes for å skape den nødvendige (og avtalte) sikkerheten rundt informasjon.

Databehandleren skal - i alle tilfeller og minst - iverksette følgende tiltak:

Systemadgang:

Alle systemer og tjenester hos Uni Micro AS er sikret med tilgangskontroller som tilfredsstillende gjeldende regelverk og egne risikovurderinger. Herunder bl.a. men ikke begrenset til brukernavn/passord, multifaktor autentisering. Alle data som Uni Micro AS oppbevarer eller håndterer på vegne av Behandlingsansvarlige sikres for å hindre uautorisert tilgang. Systemene og tjenestene har løsninger for tilgangskontroll slik at Behandlingsansvarlig selv begrense egne brukeres tilganger.

Fysisk sikkerhet:

Uni Micro skal ha tilfredsstillende fysiske sikringstiltak på alle sine lokasjoner, og der det er nødvendig vil lokasjonene være delt inn i ulike soner (for sentral infrastruktur, serverpark m.m.). Ved bruk av underleverandører vil Uni Micro AS gjennom avtaler sikre at kravet til fysisk sikring er tilfredsstillende.

Systemmessig sikkerhet:

Uni Micro AS benytter bare anerkjente underleverandører for våre løsninger. Systemer og tjenester sikres ved regelmessig testing, vurdering og evaluering, der formålet er å sikre konfidensialitet, integritet og tilgjengelighet for leverte systemer og tjenester. Alle data i løsningene er logisk separert

på klientnivå for å sikre mot uautorisert tilgang. Alle tjenester og systemer vi drifter overvåkes kontinuerlig, og hendelser håndteres løpende av driftspersonell i henhold til egne prosedyrer og rutiner. Alle data som lagres i våre skyløsninger blir regelmessig sikkerhetskopiert. I tillegg vil egne sikkerhetskopier regelmessig kopieres til en annen sekundær lokasjon.

Systemene og tjenestene har støtte for tilgangsstyring slik at den Behandlingsansvarlige selv kan, og har ansvar for, å administrere hva den enkelte bruker har tilgang til.

C.3 Lagringsperiode / sletterutine

I de tilfeller hvor det er databehandleren som oppbevarer/lagrer personopplysninger og det ikke er tilgjengeliggjort verktøy for den behandlingsansvarlige til å selv slette personopplysninger, blir personopplysningene oppbevart av databehandleren inntil den behandlingsansvarlige anmoder om å få opplysningene slettet og/eller tilbakelevert.

I de tilfeller hvor det er databehandleren som oppbevarer/lagrer personopplysninger og det er tilgjengeliggjort verktøy for den behandlingsansvarlige til selv å slette personopplysninger, blir personopplysningene oppbevart av databehandleren inntil den behandlingsansvarlige selv har hentet og/eller slettet disse.

I de tilfeller hvor databehandleren ikke oppbevarer/lagerer personopplysninger er den behandlingsansvarlige selv ansvarlig for oppbevaring og sletting av slike opplysninger.

I de tilfeller hvor databehandleren oppbevarer midlertidige kopier, f.eks. i form av backup tilsendt for hjelp/support skal disse slettes så snart som mulig etter at behovet for slike data er borte, og senest innen 10 dager, og uansett på anmodning fra den behandlingsansvarlige.

Anonymisering/Scrambling av data vil være å betrakte som sletting på lik linje med ordinær sletting.

C.4 Lokasjoner for behandling

Behandling av de i avtalen omfattede personopplysninger kan ikke uten den behandlingsansvarliges aksept skje på andre enn følgende steder:

Norge - Av Uni Micro (databehandler)

Irland – Av Microsoft Azure (underleverandør)

Andre Lokasjoner - Av andre underleverandører, som angitt i punkt C5 (under)

C.5 Instruksjoner eller godkjenning vedrørende overføring av personopplysninger til tredjeland

Databehandleren kan overføre de Personopplysningene Databehandleren behandler på vegne av den Behandlingsansvarlige til de land der Databehandleren og Underleverandørene driver sin virksomhet og lagre dem her.

Den Behandlingsansvarlige er kjent med dette og godtar denne overføringen så lenge den er nødvendig for å gjennomføre de avtalte leveransene.

Den Behandlingsansvarlige godtar at Personopplysningene kan behandles utenfor Norge. Databehandler skal likevel ikke overføre Personopplysninger til land utenfor EU/EØS-området uten et samtykke fra den Behandlingsansvarlige.

Dersom den Behandlingsansvarlige godtar en slik overføring, skal Databehandleren sørge for at overføring skjer basert på godkjente overføringsgrunnlag, jfr. GDPR artikkel 44-46.

Vedlegg D Partenes regulering av andre forhold

D.1 Vederlag for bistand til den behandlingsansvarlige, eller dennes representanter

Generelt så vil databehandler (Uni Micro AS) kunne fakturere timepris for medgått tid til bistand som beskrevet i denne avtales punkt: «Bistand til den behandlingsansvarlige», samt eventuell annen bistand relatert til personlovgivningen, med den til enhver tid gjeldende timepris for konsulentbistand.

D.2 Vederlag for verktøy/funksjonalitet

Uni Micro vil kunne tilby spesielle verktøy eller funksjonalitet for at den behandlingsansvarlige selv på en enkel måte settes i stand til å utføre operasjoner som kreves eller ønskes, etter den til enhver tid gjeldende personvernlovgivning. Uni Micro vil kunne kreve vederlag for å gi tilgang til slikt verktøy/funksjonalitet, for å dekke inn eventuelle kostnader med utvikling og vedlikehold av dette.

D.3 Særlig om Regnskapsbyrå

Denne databehandleravtalen understøtter kravspesifikasjoner for utkontraktering av system og drift, utarbeidet av Regnskap

Norge: <https://www.regnskapnorge.no/artikler/teknologi2/kravspesifikasjoner-ved-utkontraktering-av-system--og-driftsoppgaver-fra-regnskapsvirksomheten-til-andre/>