

Databehandleravtale

1. Avtalens hensikt

I henhold til General Data Protection Regulation (GDPR) art. 28.

Avtalens hensikt er å regulere rettigheter og plikter etter General Data Protection Regulation, heretter kalt «GDPR» eller forordningen. Avtalen skal sikre at personopplysninger om de registrerte ikke brukes urettmessig eller kommer uberettigede i hende.

Avtalen regulerer databehandlers (Regnskapsforetaket) bruk av personopplysninger på vegne av den behandlingsansvarlige (kunden), herunder innsamling, registrering, sammenstilling, lagring, utlevering eller kombinasjoner av disse.

Definisjonene i personvernforordningen (EU) 2016/679 artikkel 4 gjelder tilsvarende for begreper brukt i denne databehandleravtalen.

2. Behandlingens formål og art

Formålet med Regnskapsforetakets Behandling av Personopplysninger er å gjennomføre regnskapsoppdraget i samsvar med Avtalen, herunder Regnskapsforetakets standard leveransevilkår for regnskapsoppdrag ("**Standardvilkårene**").

I *Vedlegg 1* i dette dokumentet beskrives de konkrete formålene med Behandlingene, samt de kategorier Personopplysninger og Registrerte som omfattes.

Databehandleravtalen gjelder ikke for Behandling av Personopplysninger som utføres for Regnskapsforetakets egne formål. Dette omfatter også Behandlinger som er nødvendige for å oppfylle plikter som Regnskapsforetaket er pålagt gjennom lov. For slike Behandlinger er Regnskapsforetaket selv Behandlingsansvarlig.

3. Regnskapsforetakets plikter

Regnskapsforetaket skal bare Behandle Personopplysninger i tråd med dokumenterte instruksjoner fra Kunden, herunder instruksjoner gitt i Avtalen og i denne databehandleravtalens Vedlegg 1.

Dersom Regnskapsforetaket mener at en instruks fra Kunden er i strid med personvernregelverket, skal Kunden varsles om dette uten ugrunnet opphold.

Regnskapsforetaket skal uten ugrunnet opphold varsle Kunden dersom Regnskapsforetaket ikke vil være i stand til å overholde sine forpliktelser etter denne databehandleravtalen.

Regnskapsforetakets behandling av opplysninger skal skje innenfor de instruksjoner og rammer slik de er beskrevet i denne avtalen og tilknyttede lisensavtaler og brukervilkår. Regnskapsforetaket skal bistå kunden med å sikre at kravene i artikkel 32 til 36 om informasjonssikkerhet og avvikshåndtering ivaretas.

Regnskapsforetaket plikter å gi kunden tilgang til sin sikkerhetsdokumentasjon, og bistå, slik at kunden kan ivareta sitt eget ansvar etter lov og forskrift.

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

Regnskapsforetaket skal treffe alle tiltak som er nødvendige for å etablere et egnet sikkerhetsnivå ved Behandlingen, i samsvar med kravene i personvernforordningen artikkel 32. Tiltakene skal dokumenteres, og dokumentasjonen skal gjøres tilgjengelig for Kunden på forespørsel.

Regnskapsforetaket skal på forespørsel gi Kunden tilgang til all informasjon og dokumentasjon som er nødvendig for å påvise at Behandlingen skjer i samsvar med denne Avtalen og Kundens instruksjer, og skal bidra til og legge til rette for sikkerhetsrevisjoner og inspeksjoner gjennomført av Kunden eller den Kunden bemyndiger, innen rimelig tid etter forespørsel.

Dersom det avdekkes avvik, skal Regnskapsforetaket uten ugrunnet opphold iverksette korrigerende tiltak.

Regnskapsforetaket har egne rutiner for risikovurdering og oppfølging. Det gjennomføres årlig en gjennomgang av vesentlige risikoer og hvilke tiltak virksomheten har iverksatt for å håndtere disse, herunder for de systemene som omfattes av denne Avtalen.

Regnskapsforetaket skal bistå Kunden med å oppfylle Kundens plikt til å svare på henvendelser fra Registrerte som ønsker å utøve sine rettigheter etter personvernforordningen kapittel III (herunder rett til innsyn, retting, sletting mv.). Regnskapsforetaket skal ikke selv besvare slike henvendelser, men uten ugrunnet opphold videresende henvendelsen til Kunden, eller henvide den Registrerte til selv å kontakte Kunden direkte.

Regnskapsforetaket har taushetsplikt om dokumentasjon og personopplysninger som vedkommende får tilgang til iht. denne avtalen. Denne bestemmelsen gjelder også etter avtalens opphør.

Regnskapsforetaket har ikke rett til å utlevere personopplysninger til andre enn det som følger av denne avtalens punkt 4 om underleverandør, eller ved pålegg fra offentlige myndigheter samt for å oppfylle rettslige forpliktelser. I tillegg kan regnskapsforetaket utlevere opplysninger til revisor.

Regnskapsforetaket skal uten ugrunnet opphold varsle Kunden om ethvert brudd på personopplysningssikkerheten som har medført en hendelig eller ulovlig tilintetgjørelse, tap, endring, uautorisert utlevering av eller tilgang til Personopplysninger som Behandles i medhold av denne Avtalen. Varselet skal minst inneholde de opplysningene som kreves etter personvernforordningen artikkel 33 nr. 3, herunder en beskrivelse av bruddets art, sannsynlige konsekvenser og hvilke tiltak som er iverksatt eller foreslås iverksatt for å håndtere bruddet.

Regnskapsforetaket skal straks iverksette nødvendige tiltak for å hindre eller begrense konsekvensene av sikkerhetsbruddet.

Regnskapsforetaket og dens underleverandører skal kun behandle personopplysninger innenfor Norge og EU, med mindre annet er avtalt og lovlig.

4. Vilkår for bruk av andre databehandlere

Kunden gir regnskapsforetaket fullmakt til å inngå avtale om bruk av underleverandører i den utstrekning det er hensiktsmessig og forsvarlig. Regnskapsforetaket forplikter seg til å påse at underleverandører overholder samme avtalemessige forpliktelser som databehandler.

Regnskapsforetaket har p.t. avtaler med følgende underleverandører som omfattes av denne oppdragsavtalen, der behandling av personopplysninger også utføres av underleverandør.

Navn	Type behandling	Lokasjon	Land	Ytterligere sikkerhetstiltak
Sticos, Visma Software AS	Leverandør av ERP-system.	EU/ EØS	Norge	
PowerOffice, Visma Software AS	Leverandør av ERP-system.	EU/ EØS	Norge	
Tripletex, Visma Software AS	Leverandør av ERP-system.	EU/ EØS	Norge	
IT Relasjon AS	Leverandør av IT-infrastruktur, herunder drift av applikasjoner,	EU/ EØS	Norge	

	lagring og sikkerhetskopiering av data.			
Maestro , Maestro Soft AS	Leverandør av ERP-system.	EU/ EØS	Norge	
Bizview , Exsitec AS	Leverandør av rapporteringssystem	EU/ EØS	Norge	
SharePoint/OneDrive , Microsoft	Lagring, produksjonssystem	EU/ EØS	Norge	
Claude , Anthropic			USA	SCC

Før en ny underleverandør engasjeres i Behandlingen, skal Kunden gis skriftlig varsel, senest to uker før Personopplysninger overlates til den nye underleverandøren. Varaset skal inneholde opplysninger om hvor Behandlingen vil finne sted, jf. denne databehandleravtalens punkt 5.

Kunden skal kunne protestere mot at Personopplysningene overlates til nye Databehandlere. I så fall skal Partene lojalt forsøke å enes om en løsning som er akseptabel for begge Parter. Dersom dette ikke fører frem kan Avtalen sies opp av begge Parter, i samsvar med Standardvilkårene.

Regnskapsforetaket skal inngå skriftlig avtale med sine underleverandører som pålegger dem de samme forpliktelsene som Regnskapsforetaket selv har etter denne databehandleravtalen. Regnskapsforetaket er fullt ut ansvarlig overfor Kunden for den Behandlingen som underleverandøren utfører.

5. Vilkår for overføring ut av EU/EØS

Personopplysninger kan *bare* overføres til land utenfor EU/EØS-området dersom Kunden på forhånd har gitt sitt samtykke til dette, og det foreligger et gyldig overføringsgrunnlag etter personvernforordningen kapittel V (eksempelvis en adekvansbeslutning fra EU-kommisjonen, EUs standard personvernbestemmelser (SCC) eller bindende virksomhetsregler (BCR)).

Kunden samtykker til overføring ut av EU/EØS-området som skjer i forbindelse med at Personopplysninger overlates til eksisterende underleverandører som fremgår av oversikten i denne databehandleravtalens punkt 4, på de vilkår (herunder behandlingssted og overføringsgrunnlag) som er angitt der.

Som forhåndssamtykke etter denne bestemmelsen regnes også manglende innsigelse fra Kunden mot at Behandlingen overlates til en underleverandør som Behandler Personopplysninger utenfor EU/EØS-området, jf. denne databehandleravtalens punkt 4.

6. Sletting og tilbakeføring av personopplysninger

Ved Avtalens opphør plikter Regnskapsforetaket å tilbakelevere, slette eller anonymisere alle Personopplysninger i samsvar med Kundens nærmere instruks på opphørstidspunktet. Partene skal lojalt enes om den praktiske gjennomføringen av denne plikten som ivaretar begge Parter behov for å oppfylle lovpålagte krav og sikre daglig drift.

Sletteplikten gjelder uansett ikke Personopplysninger som inngår i Regnskapsførerforetakets egen oppdragsdokumentasjon, jf. denne databehandleravtalens pkt. 2.

7. Databehandleravtalens varighet og endringer

Databehandleravtalen gjelder så lenge Regnskapsforetaket behandler personopplysninger på vegne av Kunden. Taushetsplikten gjelder på ubestemt tid.

Ved brudd på denne databehandleravtalen eller personvernregelverket kan Kunden pålegge Regnskapsforetaket å stanse den videre Behandlingen av Personopplysningene med øyeblikkelig virkning.

Databehandleravtalen kan endres ved behov og enighet mellom partene i samsvar med Standardvilkårene.

8. Meddelelser og annen kommunikasjon

Meddelelser og annen kommunikasjon etter denne databehandleravtalen skal skje i samsvar med Standardvilkårene.

9. Lovvalg og verneting

Lovvalg og verneting er regulert i Standardvilkårene pkt. 15.

Vedlegg 1 Kategorier Personopplysninger og behandlingsformål

Personopplysning	Formål med opplysningen
For- og etternavn	Identifikasjon for korrekt utbetaling av lønn og godtgjørelser herunder reiseregninger og utlegg. Identifikasjon for hendelser relatert til arbeidsforholdet og identifikasjon ved annen pliktig offentlig innrapportering.
Adresse privat	Kommunikasjon.
Adresse arbeidssted	Offentlig og intern rapportering.
Statsborgerskap	A-melding og sikre korrekte ytelser og trekk.
Bostedsland	A-melding og sikre korrekte ytelser og trekk.
Telefonnummer (fast)	Kommunikasjon.
Telefonnummer (mobil)	Kommunikasjon.
E-postadresse	Kommunikasjon.
Fødselsdato / nummer	Identifikasjon for utbetaling av lønn og godtgjørelser herunder reiseregninger og utlegg, arbeidsforhold, annen pliktig offentlig innrapportering.
Kjønn	Statistikkformål for styrets årsberetning, intern rapportering mv.
Ansattnummer / ArbeidsforholdsID	A-melding. Intern identifikasjon og kategorisering for tilordning i avdeligsregnskap mv.
Kontonummer i bank	Sikre korrekt utbetaling av lønn og andre ytelser.
Sivilstatus	Sikre korrekte ytelser og trekk som påvirkes av sivilstatus.
Ektefelle, herunder navn og fødselsnummer	Sikre korrekt skattemessig innrapportering av lønnsforhold, formuesforhold mv.
Pårørendeinformasjon	Kommunikasjon med pårørende om særskilte forhold ved akutt sykdom, dødsfall mv.
Stillingsbetegnelse / yrkeskode	A-melding og sikre korrekt utbetaling lønn.
Stillingsnivå, herunder stillingsprosent og timer pr uke. Dato for siste endring.	A-melding og sikre korrekt utbetaling lønn.
Arbeidstidsordning	A-melding og sikre korrekt utbetaling lønn.

Personopplysning	Formål med opplysningen
Yrkesopplysninger av betydning for lønns og arbeidsvilkår	A-melding og sikre korrekt utbetaling lønn.
Utdannelse og praksis, herunder lønnsansiennitet.	A-melding og sikre korrekte ytelser og trekk.
Medlemskap i fagforeninger og andre yrkesrelaterte foreninger.	Sikre korrekte ytelser og trekk.
Dekket av tariffavtale, herunder lønnstrinn	Sikre korrekte ytelser og trekk.
Lønns- og provisjonsopplysninger, herunder avlønningstype og siste dato for avlønning.	A-melding og sikre korrekt utbetaling lønn.
Pensjonsopplysninger	Sikre korrekt pensjonsinnbetaling og pensjonsytelse.
Skattetrekksopplysninger	Sikre korrekt skattetrekk.
Forsikringsforhold, herunder dekningsomfang og nødvendige helseopplysninger (egenerklæringer mv)	Sikre korrekt forsikringsdekning etter avtale mellom arbeidsgiver og forsikringsselskap.
Fravær og permisjoner, herunder type og varighet.	Sikre korrekte ytelser og trekk. Offentlig innrapportering av sykepenger, permisjonsgodtgjørelse mv.
Ansettelses- og sluttdato, herunder start- og sluttdatoer ved fusjon og fisjon.	A-meldingen, lønnsberegninger og forsikringsordninger. Følge opp jubileum mv.
Sluttårsak, herunder oppsigelse og dødsfall.	Sikre korrekte ytelser og trekk. Statistiske formål.
Firmabil og andre naturalytelser	Sikre korrekt regnskapsrapportering og innberetning av fordel. Forsikringsdekningsformål.
Eierandeler i selskap	Aksjonærregstermeldinger
Rolle i selskap	Sikre korrekte ytelser og trekk. Interne rapporteringsformål. A-melding. Sikre korrekte opplysninger i årsregnskapet.
Vilkår i aksjonæravtaler	Sikre korrekt behandling aksjonærer imellom.
Eiendeler i samboerskap	Sikre korrekt innberetning av skattemessige formål.
Gjeld / fordringer overfor arbeidsgiver, herunder vilkår for mellomregningen.	Sikre korrekt inn- og utbetaling samt avregning av renter og gebyrer.
Informasjon i regnskapsdokumentasjon om ansattes atferdsmønster, herunder kjøp av varer og tjenester og bevegelsesmønster	Godtgjørelse av utlegg pådratt i næringsvirksomhet eller føring av private utgifter på privatkonto.

Kategorier av registrerte vil kunne inkludere:

- Ansatte, vikarer eller midlertidig ansatte hos Kunden
- Personlige kunder hos Kunden
- Eiere av Kundens virksomhet
- Styremedlemmer hos Kunden