

Databehandleravtale

Avtale om behandling av personopplysninger etter personvernforordningen (GDPR) artikkel 28, inngått i forbindelse med tjenesten Vaktplansjekk.

VERSJON	MALVERSJON DATERT	DOKUMENT
1.0	26.08.2026	SV-DPA-2026-1

BEHANDLINGSANSVARLIG – KUNDEN

VIRKSOMHET

ORGANISASJONSNR.

ADRESSE

KONTAKTPERSON

E-POST

DATABASEHANDLER

Steel Ventures AS

Organisasjonsnr. 935 845 823
Bergen, Norge
personvern@steel-consultancy.com
steelconsulting.no

Tjenesten leveres under forretningsnavnet
Steel Consulting Partners.

1 Avtalens formål, omfang og partenes roller

- 1.1 Denne databehandleravtalen («Avtalen») regulerer Databehandlerens behandling av personopplysninger på vegne av Behandlingsansvarlig, og oppfyller kravene i personvernforordningen (forordning (EU) 2016/679, «GDPR») artikkel 28 nr. 3, jf. personopplysningsloven (lov 15. juni 2018 nr. 38) § 1.
- 1.2 Avtalen gjelder for behandlingene som er beskrevet i **Vedlegg A**, og som utføres som ledd i tjenesten **Vaktplansjekk** — en gjennomgang av Behandlingsansvarliges vaktplaner og arbeidstidsdata mot arbeidsmiljøloven (lov 17. juni 2005 nr. 62) kapittel 10 og eventuelle allmenngjorte tariffbestemmelser etter allmenngjøringsloven (lov 4. juni 1993 nr. 58) med tilhørende forskrifter.
- 1.3 Med «**Oppdragsavtalen**» menes den skriftlige bestillingen eller avtalen om levering av Vaktplansjekk som Avtalen knytter seg til, herunder avtalt vederlag og timesatser.
- 1.4 Behandlingsansvarlig har rett til å gi og endre instruksjoner etter punkt 2 og til å føre kontroll etter punkt 9, og plikter å (i) sikre at det foreligger et gyldig behandlingsgrunnlag for behandlingen, (ii) oppfylle informasjonsplikten overfor de registrerte, (iii) minimere og pseudonymisere opplysningene før overlevering, jf. Vedlegg A, og (iv) holde kontaktopplysningene i partsfeltet oppdatert.
- 1.5 Vedlegg A, B og C utgjør en integrert del av Avtalen.
- 1.6 Ved motstrid går Avtalen foran Oppdragsavtalen og øvrige avtaler mellom partene i spørsmål som gjelder behandling av personopplysninger.

2 Instruksjonsmyndighet

- 2.1 Databehandleren skal bare behandle personopplysninger etter dokumenterte instruks fra Behandlingsansvarlig, herunder ved overføring til tredjeland, med mindre annet kreves etter EØS-retten eller norsk rett som Databehandleren er underlagt. (GDPR art. 28 nr. 3 bokstav a)
- 2.2 Dersom Databehandleren er rettslig forpliktet til å behandle personopplysninger ut over instruks, skal Behandlingsansvarlig underrettes om det rettslige kravet før behandlingen finner sted, med mindre den aktuelle retten forbyr slik underretning av hensyn til viktige samfunnsinteresser.
- 2.3 Avtalen med vedlegg, sammen med Oppdragsavtalen, utgjør Behandlingsansvarliges fullstendige instruks ved avtaleinngåelsen. Endringer i instruks skal avtales skriftlig.
- 2.4 Dersom Databehandleren mener at en instruks er i strid med GDPR eller annen personvernlovgivning, skal Databehandleren umiddelbart underrette Behandlingsansvarlig og kan avvente gjennomføring inntil instruks er bekreftet eller endret.
- 2.5 Databehandleren behandler ikke personopplysningene for egne formål. Opplysningene brukes ikke til produktutvikling, statistikk, trening av modeller, markedsføring eller andre formål ut over det som følger av Vedlegg A.
- 2.6 Mottar Databehandleren henvendelse fra Datatilsynet eller annen myndighet, eller et rettslig bindende pålegg om utlevering av personopplysninger som behandles på vegne av Behandlingsansvarlig, skal Behandlingsansvarlig varsles uten ugrunnet opphold og før utlevering, med mindre varsling er forbudt. Databehandleren skal bestrebe pålegget der det er rettslig grunnlag for det, og begrense enhver utlevering til det som er strengt nødvendig.

3 Taushetsplikt

- 3.1 Databehandleren sikrer at fysiske personer med tilgang til personopplysningene har forpliktet seg til fortrolighet eller er underlagt en egnet lovfestet taushetsplikt. (art. 28 nr. 3 bokstav b)
- 3.2 Taushetsplikten gjelder også etter at avtaleforholdet er avsluttet.
- 3.3 Tilgang gis etter tjenstlig behov, og bare til personell som er nødvendig for å levere tjenesten.

4 Informasjonssikkerhet

- 4.1 Databehandleren skal gjennomføre egnede tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som er tilpasset risikoen, jf. GDPR artikkel 32. (art. 28 nr. 3 bokstav c)
- 4.2 Tiltakene som er gjennomført på avtaletidspunktet er beskrevet i **Vedlegg B**. Databehandleren kan oppdatere tiltakene, forutsatt at sikkerhetsnivået ikke reduseres.
- 4.3 Partene legger ved avtaleinngåelsen til grunn at behandlingen har begrenset risiko, fordi opplysningene er pseudonymiserte, ikke omfatter særlige kategorier av personopplysninger etter GDPR artikkel 9, og oppbevares i et kort, avgrenset tidsrom. Endrer disse forutsetningene seg, skal tiltakene etter punkt 4.1 vurderes på nytt.

5 Underdatabehandlere

- 5.1 Behandlingsansvarlig gir med dette en generell forhåndsgodkjenning til bruk av underdatabehandlere. (art. 28 nr. 2 og nr. 3 bokstav d)
- 5.2 Underdatabehandlerne som benyttes ved avtaleinngåelsen er listet i **Vedlegg C**.
- 5.3 Databehandleren skal varsle Behandlingsansvarlig skriftlig **minst 30 dager** før en ny underdatabehandler tas i bruk eller en eksisterende erstattes. Behandlingsansvarlig kan innen varselfristen protestere på saklig grunnlag. Oppnås ikke enighet, kan Behandlingsansvarlig si opp den berørte tjenesten uten kostnad.
- 5.4 Databehandleren skal pålegge enhver underdatabehandler de samme forpliktelsene som følger av Avtalen, ved avtale eller annet rettslig dokument, og er fullt ut ansvarlig overfor Behandlingsansvarlig for underdatabehandlerens oppfyllelse. (art. 28 nr. 4)
- 5.5 Databehandleren skal på skriftlig forespørsel gi Behandlingsansvarlig innsyn i de relevante delene av avtalen med underdatabehandleren, med unntak av kommersielle vilkår.

6 Bistand til Behandlingsansvarlig

- 6.1 Databehandleren skal, så langt det er mulig, bistå Behandlingsansvarlig med egnede tekniske og organisatoriske tiltak med å oppfylle plikten til å svare på anmodninger om utøvelse av de registrertes rettigheter etter GDPR kapittel III. (art. 28 nr. 3 bokstav e)
- 6.2 Databehandleren skal bistå Behandlingsansvarlig med å oppfylle forpliktelsene etter GDPR artikkel 32–36, herunder sikkerhet, melding om brudd på personopplysningssikkerheten til tilsynsmyndigheten og underretning til de registrerte etter artikkel 33 og 34, samt eventuell vurdering av personvernkonsekvenser etter artikkel 35, tatt i betraktning behandlingens art og opplysningene Databehandleren har tilgang til. (art. 28 nr. 3 bokstav f)
- 6.3 Henvendelser fra registrerte som mottas direkte av Databehandleren skal ikke besvares på egen hånd, men videreformidles til Behandlingsansvarlig uten ugrunnet opphold og senest innen **fem virkedager**.
- 6.4 Bistand etter punktene 6.1 og 6.2 ytes uten særskilt vederlag med inntil **fem timer per kalenderår**. Bistand ut over dette faktureres etter timesatsene i Oppdragsavtalen, etter forutgående skriftlig varsel. Bistand ved brudd som skyldes Databehandlerens forhold, ytes alltid vederlagsfritt.

7 Brudd på personopplysningssikkerheten

- 7.1 Databehandleren skal varsle Behandlingsansvarlig **uten ugrunnet opphold, og normalt senest innen 48 timer**, etter å ha blitt kjent med et brudd på personopplysningssikkerheten som berører Behandlingsansvarliges personopplysninger.
- 7.2 Varselet skal så langt mulig beskrive bruddets art, kategoriene og omtrentlig antall registrerte og opplysninger som er berørt, sannsynlige konsekvenser, samt tiltak som er eller foreslås truffet. Dersom det ikke er mulig å gi all informasjon samtidig, kan opplysningene gis trinnvis uten ytterligere ugrunnet opphold.
- 7.3 Databehandleren skal uten ugrunnet opphold iverksette rimelige tiltak for å begrense og utbedre bruddet.
- 7.4 Det er Behandlingsansvarlig som melder brudd til Datatilsynet og eventuelt underretter de registrerte. Databehandleren skal bistå med nødvendig informasjon.
- 7.5 Databehandleren skal dokumentere alle brudd som berører Behandlingsansvarliges opplysninger.

8 Sletting og tilbakelevering

- 8.1 Med mindre Behandlingsansvarlig skriftlig har bedt om tilbakelevering etter punkt 8.2, slettes personopplysningene **senest 30 kalenderdager etter at rapporten er levert**, uavhengig av om avtaleforholdet fortsetter. Dette omfatter mottatte filer, e-postvedlegg og arbeidskopier.
- 8.2 Ved opphør av tjenesten skal Databehandleren, etter Behandlingsansvarliges valg, slette eller tilbakelevere alle personopplysninger og slette eksisterende kopier, med mindre lagring kreves etter EØS-retten eller norsk rett. Tilbakelevering skjer i så fall før sletting etter punkt 8.1. (art. 28 nr. 3 bokstav g)
- 8.3 Databehandleren fører en enkel slettelogg med dato for sletting og hvilket oppdrag den gjelder, og bekrefter sletting skriftlig på forespørsel.
- 8.4 Alminnelig kunderskorrrespondanse og bokføringspliktig materiale oppbevares i samsvar med bokføringsloven § 13. Den ferdige rapporten oppbevares i inntil **24 måneder** etter levering som dokumentasjon for utført oppdrag og for håndtering av reklamasjons- og ansvarskrav. Slik oppbevaring skjer med Databehandleren som behandlingsansvarlig, jf. GDPR artikkel 6 nr. 1 bokstav f, og Behandlingsansvarlig kan kreve rapporten slettet tidligere. Funn som gjenbrukes til metodeutvikling, anonymiseres slik at de ikke lenger utgjør personopplysninger.

9 Dokumentasjon og revisjon

- 9.1 Databehandleren skal gjøre tilgjengelig for Behandlingsansvarlig all informasjon som er nødvendig for å påvise at forpliktelsene i GDPR artikkel 28 er oppfylt. (art. 28 nr. 3 bokstav h)
- 9.2 Databehandleren skal muliggjøre og bidra til revisjoner, herunder inspeksjoner, som gjennomføres av Behandlingsansvarlig eller en revisor utpekt av denne. Revisjonen skal først søkes gjennomført ved at Databehandleren besvarer skriftlig egenerklæring og fremlegger relevant dokumentasjon. Stedlig inspeksjon kan kreves dersom dokumentasjonen ikke er tilstrekkelig. Revisjon varsles skriftlig minst 30 dager i forveien, gjennomføres i normal arbeidstid og høyst én gang per kalenderår med mindre det foreligger et dokumentert brudd.

- 9.3 Revisor skal ikke være en konkurrent av Databehandleren og skal undertegne taushetserklæring. Behandlingsansvarlig bærer egne og revisors kostnader samt Databehandlerens dokumenterte medgåtte tid etter timesatsene i Oppdragsavtalen, med mindre revisjonen avdekker vesentlig mislighold fra Databehandlerens side.
- 9.4 Databehandleren fører protokoll over behandlingsaktiviteter utført på vegne av Behandlingsansvarlig, jf. GDPR artikkel 30 nr. 2.

10 Overføring ut av EØS

- 10.1 Vaktplandata lagres i EØS så langt det følger av Databehandlerens konfigurasjon av de tjenestene som er listet i **Vedlegg C**. Underdatabehandleren kan i forbindelse med support, drift og sikkerhetskopiering behandle opplysninger utenfor EØS. Slik overføring skjer bare på et gyldig overføringsgrunnlag etter GDPR kapittel V, angitt i Vedlegg C.
- 10.2 Faller et overføringsgrunnlag bort, skal Databehandleren uten ugrunnet opphold etablere et alternativt grunnlag eller opphøre med overføringen.

11 Ansvar

- 11.1 Erstatningsansvar overfor registrerte følger av GDPR artikkel 82. Overtredelsesgebyr ilegges etter GDPR artikkel 83.
- 11.2 I forholdet mellom partene er Databehandlerens samlede erstatningsansvar begrenset til det vederlaget Behandlingsansvarlig har betalt for den leveransen kravet knytter seg til, og uansett oppad begrenset til **kr 150 000** samlet per kalenderår. Databehandleren svarer ikke for indirekte tap, herunder tappt fortjeneste, tap av data, omdømmetap eller overtredelsesgebyr ilagt Behandlingsansvarlig, med mindre gebyret skyldes Databehandlerens mislighold av Avtalen. Begrensningene gjelder ikke ved forsett eller grov uaktsomhet, og begrenser ikke ansvar som ikke kan begrenses etter ufravikelig rett, herunder ansvar overfor registrerte etter GDPR artikkel 82.
- 11.3 Databehandleren yter ikke juridisk rådgivning. Rapportens vurderinger erstatter ikke juridisk bistand, og Behandlingsansvarlig er ansvarlig for egne beslutninger om arbeidstidsordninger.

12 Varighet, endringer, mislighold og lovvalg

- 12.1 Avtalen gjelder fra signering og så lenge Databehandleren behandler personopplysninger på vegne av Behandlingsansvarlig. Punktene 2.5, 3, 8, 10 og 11 gjelder også etter opphør. Punkt 9 gjelder i tre år etter opphør.
- 12.2 Endringer i Avtalen skal være skriftlige og signert av begge parter. Vedlegg B og C kan likevel oppdateres ensidig av Databehandleren etter fremgangsmåten i henholdsvis punkt 4.2 og punkt 5.3. Avtalen er inngått skriftlig, herunder i elektronisk form, jf. GDPR artikkel 28 nr. 9.
- 12.3 Ved vesentlig mislighold av Avtalen kan den ikke-misligholdende part heve Avtalen ved skriftlig varsel, etter at det er gitt 30 dagers frist til å rette forholdet.
- 12.4 Varsler etter Avtalen sendes skriftlig til kontaktpunktene som er angitt i partsfeltet på side 1.
- 12.5 Avtalen er underlagt norsk rett. Tvister søkes løst i minnelighet. Vernetting er den tingretten som til enhver tid har Bergen som rettssted, for tiden Hordaland tingrett, med mindre annet er avtalt i Oppdragsavtalen.

13 Signatur

Avtalen signeres i to eksemplarer, ett til hver part. Elektronisk signatur likestilles med fysisk signatur.

FOR BEHANDLINGSANSVARLIG

FOR DATABEHANDLER – STEEL VENTURES AS

SIGNATUR

SIGNATUR

NAVN OG STILLING MED BLOKKBOKSTAV

NAVN OG STILLING MED BLOKKBOKSTAV

STED OG DATO

STED OG DATO

A Behandlingens formål, art, varighet og kategorier

Formål

Kontroll av Behandlingsansvarliges vaktplaner og arbeidstidsdata mot arbeidsmiljøloven kapittel 10 og eventuelle allmenngjorte tariffbestemmelser, samt utarbeidelse av en skriftlig rapport med funn og anbefalte utbedringer.

Behandlingens art

Innlesing, strukturering, maskinell analyse og manuell kvalitetssikring av vaktdata, samt rapportering til Behandlingsansvarlig. Behandlingen omfatter **ikke** profilering, automatiserte avgjørelser med rettsvirkning, scoring av enkeltansatte eller løpende overvåking. Funn rapporteres på plan- og avdelingsnivå, med referanse til pseudonymiserte ansattkoder der det er nødvendig for å kunne rette feilen.

Varighet

Fra opplysningene mottas til de slettes, senest 30 kalenderdager etter levert rapport (punkt 8.1). For løpende kvartalsavtaler gjelder fristen for hver enkelt leveranse.

Kategorier av registrerte

Behandlingsansvarliges arbeidstakere og innleide som inngår i de vaktplanene som leveres til kontroll.

Kategorier av personopplysninger

KATEGORI	INNHOOLD
Ansattreferanse	Pseudonymisert ansattkode fastsatt av Behandlingsansvarlig, f.eks. «ANS-014». Nøkkelen forblir hos Behandlingsansvarlig.
Arbeidstidsdata	Dato, starttid, sluttid, pauser, vakttype, planlagt og faktisk arbeidet tid, overtid.
Stillingsdata	Stillingsprosent, avdeling eller arbeidssted, og tariffområde angitt på avdelings- eller virksomhetsnivå — ikke som individuell fagforeningstilhørighet.
Fraværsmarkering	Ferie og avspasering, angitt som markering uten årsak. Sykefravær, permisjon og annet fravær som kan avdekke helseforhold, skal ikke leveres.

DATAMINIMERING – BINDENDE FOR BEGGE PARTER

Behandlingsansvarlig skal pseudonymisere vaktplanene før overlevering, og skal **ikke** sende navn, fødselsnummer, kontaktopplysninger, lønn på individnivå, sykefraværsårsak, fagforeningstilhørighet eller andre særlige kategorier av personopplysninger etter GDPR artikkel 9. Mottar Databehandleren likevel slike opplysninger, skal opplysningene slettes uten ugrunnet opphold, og Databehandleren skal varsle Behandlingsansvarlig og be om en ny, korrekt minimert leveranse.

B Tekniske og organisatoriske sikkerhetstiltak

Tiltakene under er gjennomført per 26.08.2026, jf. punkt 4.2.

OMRÅDE	TILTAK
Overlevering	Filer overleveres via delt lenke i tilgangsstyrt lagringsområde, eller via annen kryptert kanal avtalt med Behandlingsansvarlig. All overføring skjer over TLS.
Lagring	Egen, tilgangsbegrenset mappe per kunde og per oppdrag i Google Workspace. Ingen kundedata lagres i felleskataloger eller i ustrukturerte e-posttråder ut over det som er nødvendig ved mottak.
Kryptering	Kryptering under overføring (TLS) og i hvile hos underdatabehandler. Lokale enheter er diskryptert (FileVault).
Tilgangsstyring	Tilgang gis etter tjenstlig behov og er per 26.08.2026 begrenset til én navngitt person. Tofaktorautentisering er påslått på alle kontoer med tilgang. Tilgangen fjernes når oppdraget er levert.
Analyseverktøy	Den maskinelle analysen utføres lokalt på Databehandlerens diskrypterte arbeidsstasjon. Kundedata overføres ikke til eksterne analyse-, statistikk- eller KI-tjenester ut over underdatabehandlerne i Vedlegg C.
Pseudonymisering	Analysen utføres på pseudonymiserte referanser. Identifiserende opplysninger som likevel mottas, slettes uten ugrunnet opphold, jf. Vedlegg A.
Sletting	Kundemappe, mottatte filer, e-postvedlegg og arbeidskopier slettes senest 30 dager etter levert rapport. Sletting føres i slettelogg med dato.
Fortrolighet	Alle med tilgang er underlagt skriftlig taushetsplikt, jf. punkt 3.
Dokumentasjon	Protokoll over behandlingsaktiviteter etter GDPR artikkel 30 nr. 2 føres og oppdateres per oppdrag.
Brudd på personopplysningssikkerheten	Rutine for håndtering, begrensning og varsling innen fristen i punkt 7.1, med fast varslingsvei til Behandlingsansvarliges oppgitte kontaktperson.
Robusthet	Behandlingen er ikke virksomhetskritisk for Behandlingsansvarlig og krever ingen særskilt tilgjengelighetsgaranti. Underdatabehandleren leverer redundant lagring og sikkerhetskopi.

C Godkjente underdatabehandlere

Listen er gyldig per 26.08.2026. Endringer varsles etter punkt 5.3.

UNDERDATABEHANDLER	TJENESTE OG BEHANDLING	LOKASJON	OVERFØRINGSGRUNNLAG
Google Ireland Limited med Google LLC og Googles øvrige underleverandører	Google Workspace — e-post (Gmail) og fillagring (Drive). Mottak, lagring og utveksling av vaktplanfiler og korrespondanse.	Primær lagring i EU/EØS. Support, drift og sikkerhetskopiering kan innebære behandling utenfor EØS.	Googles <i>Cloud Data Processing Addendum</i> med EUs standard personvernbestemmelser (SCC).

AVGRENSNING — NETTSTEDET

Nettstedet steelconsulting.no driftes av Netlify, Inc. Personopplysninger som sendes inn via kontaktskjemaet, behandles av Steel Ventures AS som **behandlingsansvarlig** for eget nettsted, og omfattes ikke av denne avtalen. Vaktplaner sendes aldri gjennom nettstedet. Se personvernerklæringen på steelconsulting.no/personvern.

Steel Ventures AS · org.nr 935 845 823 · Bergen, Norge
Tjenesten leveres under forretningsnavnet Steel Consulting Partners.

personvern@steel-consultancy.com
steelconsulting.no/personvern
SV-DPA-2026-1 · versjon 1.0