Databehandleravtale

Versjon 251103
Ajour per 3. nov 2025

Innhold

Veiledning:

GDPR er en forkortelse for *The General Data Protection Regulation*.
Databehandler er den som behandler personopplysninger på oppdrag fra den behandlingsansvarlige. Dette er vanligvis en virksomhet.
Behandlingsansvarlig er den som bestemmer formålet med behandlingen av personopplysninger og hvilke hjelpemidler som skal brukes. Dette er vanligvis en virksomhet.

.
https://www.datatilsynet.no/
https://www.regjeringen.no/no/tema/statlig-forvaltning/personvern/nye-personvernregler-i-eu/id2340094/

1. BAKGRUNN OG FORMÅL

1.1 Dette databehandlingssupplementet ("Databehandleravtalen") er en del av gjeldene hovedavtale mellom Kunde (den "Behandlingsansvarlige") og Proresult ("Databehandleren"), der begge utgjør en "Part", samlet benevnt som "Partene".

1.2 Formålet med denne Databehandleravtalen er å fastlegge Partenes rettigheter og plikter vedrørende Databehandlerens behandling av personopplysninger på vegne av den Behandlingsansvarlige under Hovedavtalen.

1.3 Med unntak for det som er spesifisert her, skal Hovedavtalens betingelser gjelde.

2. DEFINISJONER

2.1 I denne Databehandleravtalen skal følgende ord og uttrykk og ha den betydning som er angitt nedenfor.

2.2 "Gjeldende personvernregler": Gjeldende lover og regler om personvern, inkludert personopplysningsloven og GDPR (fra og med 25. mai 2018).

2.3 "GDPR": EUs personvernforordning 2016/679.

2.4 "Standardklausuler": Standard Contractual Clauses (SCCs) vedtatt av EU-kommisjonen i henhold til GDPR artikkel 46(2)(c), og/eller standard databehandleravtaler vedtatt av EU-kommisjonen eller relevant tilsynsmyndighet i henhold til GDPR artikkel 28(7) eller 28(8).

2.5 "Underdatabehandler": En annen databehandler engasjert av Databehandleren.

2.6 "Tredjestat": Et land utenfor EØS som EU-kommisjonen ikke har fastslått at sikrer et tilstrekkelig beskyttelsesnivå.

2.7 For øvrig skal ord og uttrykk og ha samme mening som de er tillagt i GDPR.

3. OMFANG

3.1 Denne Databehandleravtalen skal, så langt den passer, også omfatte behandling av data som ikke er personopplysninger, som Databehandleren har mottatt, er gitt tilgang til eller har generert i forbindelse med Hovedavtalen. Begrepet "personopplysninger" skal, så langt det passer, derfor også omfatte data som ikke er personopplysninger.

3.2 Databehandlingens formål og art, typen personopplysninger som behandles, samt kategorier av registrerte fremgår av Vedlegg 1.

4. GENERELLE PLIKTER

4.1 Databehandleren garanterer å ha gjennomført egnede tekniske og organisatoriske tiltak som sikrer at behandlingen oppfyller kravene i henhold til gjeldende personvernregler og ivaretar de registrertes rettigheter, og at disse tiltakene vil etterleves i hele avtaleperioden.

4.2 Databehandleren skal behandle personopplysningene utelukkende for det formål og innenfor det omfang som er angitt i Vedlegg 1 og for øvrig i samsvar med den Behandlingsansvarliges dokumenterte instrukser.

4.3 Databehandleren skal omgående underrette den Behandlingsansvarlige skriftlig hvis den har rimelig grunn til å tro at (i) en instruks fra den Behandlingsansvarlige kan medføre at Databehandleren bryter med gjeldende personvernlovgivning, eller (ii) gjeldende rett i EØS-området krever at Databehandleren behandler personopplysninger utover omfanget av den Behandlingsansvarliges dokumenterte instrukser, med mindre denne rett av hensyn til viktige samfunnsinteresser forbyr slik underretning (i så fall skal Databehandleren underrette den Behandlingsansvarlige så snart retten tillater det). I tilfelle av (i) eller (ii) skal Partene i god tro diskutere hvordan problemet kan løses uten at det negativt påvirker vernet av de registrertes rettigheter.

4.4 Hvis Databehandleren er underlagt godkjente atferds normer i henhold til GDPR artikkel 40 eller en godkjent sertifiseringsmekanisme i henhold til GDPR artikkel 42, garanterer Databehandleren at den vil etterleve slike atferds normer eller sertifiseringsmekanismer.

5. BISTAND TIL DEN BEHANDLINGSANSVARLIGE

5.1 Databehandleren skal, ved hjelp av egnede tekniske og organisatoriske tiltak, bistå den Behandlingsansvarlige i den grad det er mulig med å oppfylle den Behandlingsansvarliges plikt til å svare på anmodninger som den registrerte inngir med henblikk på å utøve sine rettigheter fastsatt i GDPR kapittel 3, herunder anmodninger om informasjon, innsyn, korrigering, sletting, begrensning av behandlingen, dataportabilitet, innsigelser, og det å ikke være underlagt automatiserte individuelle avgjørelser.

5.2 Med hensyn til behandlingens art og den informasjon som er tilgjengelig for databehandleren, skal Databehandleren bistå den Behandlingsansvarlige med forpliktelsene i henhold til GDPR artikkel 32 til 36, herunder forpliktelsene til datasikkerhet (som nærmere beskrevet i punkt 6), melding om brudd på personopplysningssikkerhet (som nærmere beskrevet i punkt 9), vurdering av personvernkonsekvenser, samt forhåndsdrøftinger.

5.3 Databehandleren skal ikke kommunisere direkte med de registrerte eller med tilsynsmyndigheter med mindre dette er forhåndsgodkjent av den Behandlingsansvarlige. Databehandleren skal umiddelbart videresende til den Behandlingsansvarlige forespørsler eller klager som den eventuelt mottar fra de registrerte. Databehandleren skal også umiddelbart videresende eventuelle forespørsler fra en tilsynsmyndighet som gjelder inspeksjoner, undersøkelser, eller tilgang til eller informasjon om personopplysninger, med mindre loven forbyr det (i så fall skal Databehandleren underrette den Behandlingsansvarlige så snart loven tillater det).

6. TEKNISKE OG ORGANISATORISKE SIKKERHETSTILTAK

6.1 Databehandleren skal gjennomføre egnede tekniske og organisatoriske sikkerhetstiltak for å verne personopplysningene mot utilsiktet eller ulovlig tilintetgjøring, tap, endring, ikke-autorisert utlevering eller tilgang. Databehandleren skal som et minimum gjennomføre de tiltakene som er påkrevd i henhold til GDPR artikkel 32, samt de tiltak som er angitt eller referert til i Vedlegg 2.

6.2 Databehandleren skal ikke utlevere eller tilgjengelig gjøre personopplysninger for tredjeparter uten skriftlig forhåndsgodkjennelse fra den Behandlingsansvarlige, med unntak for eventuelt godkjente underdatabehandlere i den utstrekning de har behov for opplysningene for å kunne utføre sine oppgaver.

6.3 Databehandleren skal påse at alle personer som er autorisert til å behandle personopplysningene har forpliktet seg til å behandle opplysningene fortrolig eller er underlagt en egnet lovfestet taushetsplikt. Databehandleren skal etter anmodning fra den behandlingsansvarlige kunne påvise at de

aktuelle personene underlagt databehandlerens instruksjonsmyndighet er underlagt ovennevnte taushetsplikt.

7. BRUK AV UNDERDATABEHANDLERE

7.1 Den Behandlingsansvarlige tillater at Databehandleren engasjerer underdatabehandlere. På forespørsel skal den Behandlingsansvarlige motta informasjon om hvem underdatabehandlerne er, samt hvor de behandler personopplysningene. Databehandleren skal underrette den Behandlingsansvarlige om eventuelle planer om å benytte andre underdatabehandlere eller skifte ut underdatabehandlere. Den Behandlingsansvarlige har rett til å motsette seg slike endringer.

7.2 I henhold til punkt 7.1 skal Databehandleren kun engasjere underdatabehandlere som gjennomfører egnede tekniske og organisatoriske tiltak som sikrer at databehandlingen oppfyller kravene etter gjeldende personvernregler og som sikrer de registrertes personvern. Databehandleren skal gjennomføre egnede kontroller av underdatabehandlerne for å verifisere deres databeskyttelsesnivå. Databehandleren skal fremlegge rapporter fra slike kontroller for den Behandlingsansvarlige.

7.3 Databehandleren skal inngå skriftlig avtale med hver underdatabehandler som pålegger egne forpliktelser med hensyn til vern av personopplysninger. Når underdatabehandleren er engasjert for å utføre spesifikke databehandlingsaktiviteter på vegne av den Behandlingsansvarlige, skal den Behandlingsansvarlige ved skriftlig avtale pålegge underdatabehandleren de samme forpliktelsene med hensyn til vern av personopplysninger som fastsatt i denne Databehandleravtalen. På forespørsel fra den Behandlingsansvarlige skal Databehandleren fremlegge kopi av avtaler med underdatabehandlere. Forretningsmessig og annen forretningssensitiv informasjon kan dog sladdes.

7.4 Databehandleren har fullt ansvar for underdatabehandlerens utførelse av sine forpliktelser.

8. INTERNASJONAL DATAOVERFØRING

8.1 Databehandleren kan kun overføre personopplysninger til en tredjestat eller en internasjonal organisasjon etter dokumenterte instrukser fra den Behandlingsansvarlige. Den Behandlingsansvarlige kan imidlertid gjøre dette hvis det kreves i henhold til gjeldende rett i EØS-området. I slike tilfeller skal den Behandlingsansvarlige underrette Databehandleren om nevnte rettslige krav før overføringen, med mindre denne rett av hensyn til viktige samfunnsinteresser forbyr slik underretning (i så fall skal Databehandleren underrette den Behandlingsansvarlige så snart retten tillater dette).

8.2 Dersom bruk av en godkjent underdatabehandler krever overføring av personopplysninger til en tredjestat, og slike overføringer er godkjent av Databehandleren, gir den Benhandlingsansvarlige Databehandleren fullmakt til å inngå standardklausuler i uendret form med underdatabehandleren på vegne av den Behandlingsansvarlige dersom dette er nødvendig for å tilfredsstille krav etter gjeldende personvernregler. Så snart en slik avtale er inngått skal underdatabehandleren fremlegge en kopi av denne for den Behandlingsansvarlige. Alle slike standardklausuler skal automatisk opphøre ved opphøret av denne Databehandleravtalen.

9. BRUDD PÅ PERSONOPPLYSNINGSSIKKERHETEN

9.1 Databehandleren skal gi skriftlig melding til den Behandlingsansvarlige om eventuelle brudd på denne Databehandleravtalen eller personopplysningssikkerheten. Meldingen skal gis senest 72 timer etter at Databehandleren ble oppmerksom på bruddet. Daglig leder hos databehandler eller den som er utpekt skal varsle den Behandlingsansvarlige. Internt skal bruddet håndteres som et avvik.

9.2 Melding om brudd på personopplysningssikkerheten må minst, i den grad det er relevant:

a) beskrive arten av bruddet, herunder, når det er mulig, kategoriene av og omtrentlig antall registrerte som er berørt, og kategoriene av og omtrentlig antall personopplysningsposter som er berørt;
b) inneholde, når det er mulig, de berørte registrertes identitet;
c) formidle navn og kontaktinformasjon til personvernrådgiveren eller et annet kontaktpunkt hos

Databehandleren for ytterligere innhenting av informasjon;
d) beskrive de sannsynlige konsekvensene av bruddet på personopplysningssikkerheten;
e) beskrive de tiltak som er truffet eller foreslått for å håndtere bruddet, herunder, dersom det er relevant, tiltak for å redusere eventuelle skadevirkninger;
f) inkludere annen informasjon som kreves for at den Behandlingsansvarlige kan overholde gjeldende personvernregler.

9.3 Databehandleren skal så snart som mulig gjennomføre alle tiltak som beskrevet i punkt e. ovenfor, samt gjennomføre alle de tiltak som med rimelighet kreves for å unngå at det senere oppstår lignende brudd på personopplysningssikkerheten. Databehandleren skal tillate den Behandlingsansvarlige å undersøke, fastlegge årsaken til og å verifisere de tiltak som er gjennomført eller foreslått av den Behandlingsansvarlige for å håndtere bruddet på personopplysningssikkerheten. Databehandleren skal, så langt det er mulig, rådføre seg med den Behandlingsansvarlige med hensyn til de tiltak som skal gjennomføres samt overveie innspill fra den Behandlingsansvarlige i den forbindelse.

9.4 Kun den Behandlingsansvarlige har rett til å informere den relevante tilsynsmuligheten og de berørte registrerte om brudd på personopplysningssikkerheten. Databehandleren skal avstå fra å informere allmennheten eller tredjepart om brudd på personopplysningssikkerheten.

10. REVISJON

10.1 Databehandleren skal dokumentere, samt gjøre tilgjengelig for den Behandlingsansvarlige, informasjon som er nødvendig for å påvise etterlevelse av denne Databehandleravtalen og gjeldende personvernregler.

10.2 Databehandleren skal muliggjøre og bidra ved revisjoner av Databehandlerens behandlingsaktiviteter som utføres av den Behandlingsansvarlige eller av annen inspektør på fullmakt fra den Behandlingsansvarlige. Databehandleren skal også muliggjøre og bidra ved revisjoner fra tilsynsmyndigheter.

10.3 Databehandleren kan, på egen hånd eller via annen inspektør på fullmakt fra Databehandleren, foreta revisjoner av sine behandlingsaktiviteter. Databehandleren skal oversende kopi av revisjonsrapporter fra slike revisjoner til den Behandlingsansvarlige. Den Behandlingsansvarlige skal ha rett til å fremlegge slike revisjonsrapporter til sine eksterne revisorer og tilsynsmyndigheter.

10.4 Databehandleren skal umiddelbart varsle den Behandlingsansvarlige hvis den mottar forespørsel fra en myndighet om å utlevere personopplysninger som er behandlet under denne Databehandleravtalen. Med mindre loven krever det, skal Databehandleren ikke etterkomme en slik forespørsel uten skriftlig forhåndsgodkjenning fra den Behandlingsansvarlige.

10.5 Dersom en revisjon avdekker avvik fra forpliktelsene i denne Databehandleravtalen, skal Databehandleren så snart som mulig avhjelpe slike avvik (og, hvis relevant, påse at den relevante underdatabehandleren gjør det samme). Den Behandlingsansvarlige kan kreve at hele eller deler av behandlingsaktivitetene midlertidig opphører til vellykket utbedring er bekreftet.

10.6 Hver av partene dekker sine egne kostnader forbundet med en revisjon. Hvis en revisjon avdekker ikke-uvesentlige avvik fra forpliktelsene i denne Databehandleravtalen, skal alle kostnader forbundet

med revisjonen dekkes av Databehandleren, herunder den Behandlingsansvarliges og eksterne revisorers rimelige kostnader.

11. ANSVARSBEGRENSNING

11.1 Databehandleren skal holde den Behandlingsansvarlige skadesløs fra eventuelle kostnader (herunder rimelige saksomkostninger) og tap som følge av et krav fra en tredjepart (inkludert tilsynsmyndigheter og registrerte) om at behandlingen av personopplysningene innebærer brudd på gjeldende personvernregler, og kravet skyldes Databehandlerens mislighold av sine forpliktelser i denne Databehandleravtalen, herunder behandling av personopplysninger utover den Behandlingsansvarliges skriftlige instrukser.

11.2 Skadesløsholdelsen er betinget av (i) at den Behandlingsansvarlige umiddelbart varsler Databehandleren om kravet, og (ii) at Databehandleren får mulighet til å samarbeide med den Behandlingsansvarlige i forsvaret mot og oppgjøret av kravet.

12. ANDRE BEHANDLINGSANSVARLIGE

12.1 Databehandleren anerkjenner at personopplysningene også behandles på vegne av den Behandlingsansvarliges konsernselskaper/kunder/klienter. Slike andre behandlingsansvarlige kan håndheve denne Databehandleravtalen som om de var avtaleparter. Slik håndheving skal imidlertid skje gjennom den Behandlingsansvarlige som er avtalepart.

12.2 Den Behandlingsansvarlige kan videresende enhver instruks fra slike andre behandlingsansvarlige, og Databehandleren skal handle i samsvar med slike instrukser som om de var den Behandlingsansvarliges egne.

12.3 Den Behandlingsansvarlige kan videresende enhver dokumentasjon og informasjon mottatt av Databehandleren til slike andre behandlingsansvarlige.

13. VARIGHET OG OPPSIGELSE

13.1 Denne Databehandleravtalen gjelder så lenge Databehandleren behandler personopplysninger på vegne av den Behandlingsansvarlige i forbindelse med Hovedavtalen.

13.2 Ved opphør eller oppsigelse av Databehandleravtalen skal Databehandleren, dersom den Behandlingsansvarlige ønsker det, slette eller tilbakelevere alle personopplysninger til den Behandlingsansvarlige og slette eksisterende kopier, og bekrefte overfor den Behandlingsansvarlige at dette er gjort, med mindre gjeldende rett i EØS-området krever at Databehandleren lagrer personopplysningene (i så fall skal Databehandleren besørge sikker lagring, men ikke aktivt behandle, personopplysningene, og skal slette personopplysningene så snart loven tillater dette).

VEDLEGG 1: DATABEHANDLINGENS OMFANG

Behandlingens formål
Formålet med databehandlingen er at Databehandleren skal kunne utføre sine forpliktelser i henhold til Hovedavtalen.

Behandlingens art og hensikt
Programvaren Proresult brukes i hovedsak til følgende:

- Administrere opplysninger om ansatte, prosjekt og kunder
- Registrering av timer, sjekklister, avvik, ferie, fravær og annen relevant informasjon
- Fakturering og lønnsutbetaling
- Rapportering (basert på ovennevnte punkt)

Varighet
Databehandlerens behandling av personopplysninger på vegne av den behandlingsansvarlige kan begynne etter at Vilkårene har tredd i kraft. Behandlingens varighet er så lenge kundeforholdet varer.

Kategorier av registrerte
Den Behandlingsansvarliges nåværende, tidligere og potensielle ansatte og kunder.

Typen personopplysninger

Diverse personalia
Navn, kjønn, fødselsdato, telefonnummer, adresse, epostadresse, funksjoner/stilling, ansatt-ID, tjenestetid, lønn, utdannelse og andre yrkesmessige kvalifikasjoner, info om pårørende, bankopplysninger, GEO lokaliseringsdata.

Andre opplysninger
Arbeidstider, prosjekt som er jobbet på, antall timer arbeidet, ferie, fravær, sykdom og HMS avvik. Systemet er også lagt opp slik at behandlingsansvarlig kan legge inn opplysninger utover det som er nevnt over.

VEDLEGG 2: TEKNISKE OG ORGANISATORISKE SIKKERHETSTILTAK

Databehandleren skal som et minimum gjennomføre alle de tiltak som er angitt eller henvist til nedenfor. Databehandleren kan ikke uten skriftlig samtykke fra den Behandlingsansvarlige gjøre endringer i disse tiltakene som reduserer graden av datasikkerhet. Databehandleren skal kontinuerlig arbeide for å forbedre sikkerhetstiltakene og sørge for at de oppdateres i takt med den teknologiske utviklingen.

Pseudonymiseringstiltak
Det er tilrettelagt funksjonalitet for pseudonymisering i programvaren. På forespørsel fra Behandlingsansvarlig vil Databehandler ytterligere kunne anonymisere nærmere angitte personer og data tilknyttet disse.

Krypteringstiltak
All kommunikasjon i løsningen skjer kryptert over HTTPS-protokollen, slik at ikke et mellomledd i nettet skal kunne lese av kommunikasjonen. Også backup går kryptert.
På lagring på serversiden krypteres alt av passord som brukerne setter selv, slik at disse ikke er lesbare for noen. Sensitive persondata har tilsvarende i størst mulig grad ekstra kryptering ved lagring.

Tiltak for å sikre personopplysningenes fortrolighet
Det er en rekke tiltak i løsningen for å sikre at det kun er brukere hos kunden og de nødvendige superbrukere hos Proresult som har tilgang til dataene til kunden. For superbrukerne er det lagt opp to-faktor-autentisering som ekstra sikkerhet, i tillegg til interne rutiner og retningslinjer hos Proresult

Tiltak for å sikre personopplysningenes integritet
Endringer i data kan kun gjøres av autoriserte brukere gjennom systemets grensesnitt. Rolle- og tilgangsstyring hindrer uautorisert endring eller sletting av data. Systemet har innebygde valideringsmekanismer som sikrer at data registreres og lagres i korrekt format. Det er etablert rutiner for testing og kvalitetskontroll ved systemoppdateringer for å hindre feil som kan påvirke data.

Tiltak for å sikre tilgjengeligheten til personopplysningene
Databasen speiles kontinuerlig (kryptert). I tillegg kjøres det backup av database hver natt som er tilgjengelig inntil to måneder tilbake i tid som også kan benyttes ved behov for tilbakestilling e.l.

Tiltak for å sikre robusthet i behandlingssystemene og -tjenestene
Databasespeilingen sikrer en mulighet for hurtig gjenoppretting om første server feiler. Tilleggsbackupen sikrer mulighet til å håndtere ulike scenario av datatap både hos enkeltkunde og totalt sett for systemet

Andre datasikkerhetstiltak:
Proresult benytter eksternt verktøy for overvåking av tjenesten. I tillegg til oppetid, overvåkes en rekke detaljer i tjenesten som skal sannsynliggjøre at Proresult kan agere på treghet, feil i deler av systemet samt forsøk på uautorisert tilgang til systemet.

VEDLEGG 3: GODKJENTE UNDERDATABEHANDLERE

Ved Vilkårenes ikrafttredelse godkjenner den behandlingsansvarlige bruken av følgende underdatabehandlere:

Navn på under-databehandler	**Adresse (hovedkontor)**	**Behandlings-sted (lokasjon for data-behandling)**	**Formål og beskrivelse av behandlingen**
Google Cloud	Velasco Clanwilliam Place, Dublin 2, Ireland	EU	Leverandør av skytjenester og infrastruktur benyttet til drift, lagring og behandling av data
Mailgun	112 E. Pecan St. #1135,San Antonio, TX 78205,US	EU	Leverandør av løsning for utsendelse av automatiske (transaksjonelle) e-poster til brukere/kunder.
SMS Teknik	Uddarne Industriväg 6SE 455 35 MUNKEDAL	Norge/ Sverige	Leverandør av løsning for utsendelse av automatiske (transaksjonelle) SMS-meldinger til brukere/kunder.
Microsoft	Dronning Eufemias Gate 71, 0194,Oslo, Norway	EU/Norge	Leverandør av skytjenester, infrastruktur og kontorløsninger (Azure, Microsoft 365) benyttet til lagring, drift og kommunikasjon.
HubSpot	HubSpot Ireland Ltd, 1 Sir John Rogerson's Quay Dublin 2 Ireland	EU	Leverandør av system for kundeadministrasjon (CRM), kundeservice, markedsføring, salg og drift av kunnskapsbase.