Innhold i Databehandleravtale

Sist oppdatert: 01.04.2025

Hver omtalt som en «part» eller sammen som «partene»

Har avtalt de følgende standard kontrakts bestemmelser (Kontrakts bestemmelsene) for å oppfylle kravene i GDPR og for vern av den registrertes rettigheter.

1 Innhold

2 Innledning

1. Disse standard kontraktbestemmelser (Kontraktbestemmelsene) regulerer rettigheter og plikter for behandlingsansvarlig og databehandler, når det behandles personopplysninger på vegne av den behandlingsansvarlige.

2. Kontraktbestemmelsene er utformet for å sikre partenes overholdelse med artikkel 28(3) i Europaparlaments- og rådsforordning (EU) 2016/679 av 27. april 2016 om vern av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger samt om oppheving av direktiv 95/46/EF (generell personvernforordning - GDPR).

3. I forbindelse med leveranse av digitale kurs, kursportal, BHT-portal, HMS system, HR system og tilhørende støttemoduler innen timeregistrering, sykefraværsregistrering og prosjektstyring samt bedriftshelsetjenester (BHT), vil databehandleren behandle personopplysninger på vegne av den behandlingsansvarlige i henhold til Kontraktbestemmelsene. Denne avtalen vil også gjelde for alle øvrige tjenester levert av Grønn Jobb som for eksempel konsulentoppdrag og bistand til søknader innenfor renhold og bygg – godkjenningsordninger.

4. Kontraktbestemmelsene skal ha forrang over andre tilsvarende bestemmelser i andre avtaler mellom partene.

5. Tre vedlegg er inntatt i Kontraktbestemmelsene og anses som omfattet av Kontraktbestemmelsene.

6. Vedlegg A inneholder detaljer om behandlingen av personopplysninger, herunder behandlingens formål og art, typen personopplysninger, kategorier av registrerte og varigheten av behandlingen.

7. Vedlegg B inneholder den behandlingsansvarliges vilkår for databehandlerens bruk av underdatabehandlere og en liste over underdatabehandlere godkjent av den behandlingsansvarlige.

8. Vedlegg C inneholder den behandlingsansvarliges instrukser for behandlingen av personopplysninger, minimum sikkerhetstiltak som skal implementeres av databehandleren og hvordan revisjoner av databehandleren og eventuelle underdatabehandlere skal gjennomføres.

9. Kontraktbestemmelsene sammen med vedleggene skal mottas skriftlig, inkludert elektronisk, av begge parter.

10. Kontraktbestemmelsene skal ikke frita databehandleren fra plikter som databehandleren skal følge etter personvernforordningen (GDPR) eller annen lovgivning.

3 Behandlingsansvarliges rettigheter og plikter

1. Den behandlingsansvarlige er ansvarlig for å sikre at behandlingen av personopplysninger utføres i samsvar med GDPR (se artikkel 24 i GDPR), personvernreglene i gjeldende EU eller Medlemsstats[1] personvernregler og Kontraktbestemmelsene.

2. Den behandlingsansvarlige har rett og plikt til å fatte beslutninger om formålene med og midlene for behandlingen av personopplysninger.

3. Den behandlingsansvarlige skal være ansvarlig, for blant annet, å sikre at behandlingen av personopplysninger, som databehandleren er instruert om å utføre, har et rettslig grunnlag.

4. Behandlingsansvarlig er ansvarlig for å kun lagre å bruke opplysninger i den utstrekning, og til de formål som er nødvendig for utføre behandlingene.

5. Behandlingsansvarlig er ansvarlig for at egendefinerte datafelt verken i seg selv, eller med dets innhold bryter med den til enhver tid gjeldende lov for personopplysninger. Det samme gjelder bruk av kombinasjoner av datafelter i for eksempel rapporter mv.

6. Der hvor systemet inneholder tekster, data eller annen informasjon som eies/disponeres av behandlingsansvarlig, innestår behandlingsansvarlig for at denne har full eiendoms- eller disposisjonsrett til slike data, og at verken lagring eller den aktuelle bruken av dette materialet innebærer en krenkelse av den registrertes rettigheter eller strider mot lov, forskrift eller andre rettsregler.

7. Ettersom databehandler ikke har direkte tilgang til systemet etter overlevering er behandlingsansvarlig ansvarlig for håndtering av henvendelser fra de registrerte om innsyn, retting og sletting mv. Dette gjelder også for tjenester utenfor systemet, herunder godkjenninger til bygg og renhold, bistand med tilsynsrapporter, samt digitale kurs og tilgang til Fagbanken. Databehandler utfører de instrukser som behandlingsansvarlig krever for å oppfylle de registrertes rettigheter i tråd med punkt 4 og 9, samt vedlegg C i denne avtalen.

4 Databehandleren skal handle etter instrukser

1. Databehandleren skal behandle personopplysninger bare på dokumenterte instrukser fra den behandlingsansvarlige, med mindre det kreves i henhold til unionsretten eller Medlemsstatenes nasjonale rett som databehandleren er underlagt. Slike instrukser skal være spesifisert vedlegg A og C. Senere instrukser kan også gis av den behandlingsansvarlige i løpet av behandlingen av personopplysninger, men slike instrukser må ikke vesentlig avvike fra gjeldende standard, gå utenfor systemets rammer, eller innebære en utilbørlig ulempe for databehandler. I slike tilfeller kan databehandler motsette seg behandlingen frem til eventuelle kostnader av slike behandlinger er dekket av behandlingsansvarlig.

2. Databehandleren skal omgående underrette den behandlingsansvarlige dersom vedkommende mener at en instruks gitt av den behandlingsansvarlige er i strid med

[1] Henvisning til "Medlemsstat" i Kontraktbestemmelsene skal forstås som henvisning til EØS-medlemsstater.

GDPR eller andre bestemmelser om vern av personopplysninger i unionsretten eller Medlemsstatenes nasjonale rett.

5 Konfidensialitet

1. Databehandleren skal kun gi tilgang til personopplysninger som behandles på vegne av den behandlingsansvarlige til personer som er under databehandlerens myndighet og som er forpliktet til konfidensialitet eller er underlagt egnet lovfestet taushetsplikt og kun til de som har nødvendig behov for tilgang. Listen over personer som har tilgang til personopplysningene skal regelmessig gjennomgås. Som følge av gjennomgang skal tilgang til personopplysningene bli trukket tilbake dersom slik tilgang ikke lenger er nødvendig for personene.
2. Databehandleren skal på anmodning fra den behandlingsansvarlige påvise at de involverte personene under databehandlerens myndighet er omfattet av ovennevnte konfidensialitetsplikt.

6 Sikkerhet ved behandlingen

1. Artikkel 32 i GDPR angir at, idet det tas hensyn til den tekniske utviklingen, gjennomføringskostnadene og behandlingens art, omfang, formål av behandlingen og sammenhengen den utføres i, samt risikoene av varierende sannsynlighets- og alvorlighetsgrad for fysiske personers rettigheter og friheter, skal den behandlingsansvarlige og databehandleren gjennomføre egnede tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som er egnet med hensyn til risikoen.

   Den behandlingsansvarlige skal vurdere risikoen til rettigheter og friheter for fysiske personer som omfattes av behandling og implementere tiltak for å redusere risikoen. Avhengig av relevans, kan slike tiltak omfatte følgende:

   a. Pseudonymisering og kryptering av personopplysninger,

   b. evne til å sikre vedvarende konfidensialitet, integritet, tilgjengelighet og robusthet i behandlingssystemene og -tjenestene,

   c. evne til å gjenopprette tilgjengeligheten og tilgangen til personopplysninger i rett tid dersom det oppstår en fysisk eller teknisk hendelse,

   d. en prosess for regelmessig testing, analysering og vurdering av hvor effektive behandlingens tekniske og organisatoriske sikkerhetstiltak er.

2. I henhold til artikkel 32 i GDPR, skal databehandleren også – uavhengig fra den behandlingsansvarlige – vurdere risikoen til rettigheter og friheter for fysiske personer som omfattes av behandlingen og implementere tiltak for å redusere risikoen. For dette formål skal den behandlingsansvarlige tilveiebringe databehandleren med all informasjon som er nødvendig for å identifisere og vurdere slik risiko.
3. Videre skal databehandleren bistå den behandlingsansvarlige i å sikre overholdelse av den behandlingsansvarliges plikter etter artikkel 32 i GDPR, ved å bl.a. å sørge for at den behandlingsansvarlige får informasjon om tekniske og organisatoriske tiltak som er implementert av databehandleren i henhold til artikkel 32 i GDPR sammen med all

annen informasjon som er nødvendig for den behandlingsansvarlige til å overholde dennes plikter under artikkel 32 i GDPR. Dersom behandlingsansvarlig initierer revisjon av databehandler for å dokumentere oppfyllelse av dette kravet skal alle kostnader knyttet til revisjonen dekkes av behandlingsansvarlig.

Dersom det i ettertid – ved vurderingen foretatt av den behandlingsansvarlige – viser seg at reduksjon av den identifiserte risiko krever implementering av ytterligere tiltak av databehandleren enn de tiltak som allerede er implementert av databehandleren etter artikkel 32 i GDPR, skal den behandlingsansvarlige spesifisere disse ytterligere tiltak som skal implementeres i Vedlegg C.

7 Bruk av underdatabehandlere

1. Databehandleren skal overholde kravene inntatt i artikkel 28(2) og (4) i GDPR for å engasjere en annen databehandler (en underdatabehandler).

2. Databehandleren skal derfor ikke engasjere annen databehandler (underdatabehandler) for oppfyllelse av Kontraktbestemmelsene uten at det på forhånd er innhentet generell skriftlig tillatelse fra den behandlingsansvarlige.

3. Databehandleren er gitt generell tillatelse fra den behandlingsansvarlige for å engasjere underdatabehandlere. Databehandleren skal skriftlig underrette den behandlingsansvarlige om eventuelle planer om å benytte andre underdatabehandlere eller skifte ut underdatabehandlere minst 3 uker på forhånd, og dermed gi den behandlingsansvarlige muligheten til å motsette seg slike endringer før underdatabehandler(e) engasjeres. Ytterligere tid for underrettelse for spesifikk underdatabehandling kan inntas i Vedlegg B. Liste over underdatabehandlere som allerede er godkjent av den behandlingsansvarlige kan inntas i Vedlegg B.

4. Dersom databehandleren engasjerer en underdatabehandler for å utføre spesifikke behandlingsaktiviteter på vegne av den behandlingsansvarlige, skal de samme forpliktelsene som er fastsatt i Kontraktbestemmelsene bli pålagt underdatabehandleren ved avtale eller et annet rettslig dokument i henhold til unionsretten eller Medlemsstatenes nasjonale rett, der det særlig gis tilstrekkelige garantier for at det vil bli gjennomført tekniske og organisatoriske tiltak som sikrer at behandlingen oppfyller kravene i Kontraktbestemmelsene og GDPR.

   Databehandleren skal derfor være ansvarlig for at underdatabehandleren minimum overholder de forpliktelser som databehandleren er pålagt etter Kontrakts bestemmelsene og GDPR.

5. En kopi av slik underdatabehandleravtale og etterfølgende endringer skal – på den behandlingsansvarliges forespørsel – oversendes den behandlingsansvarlige, og dermed gi den behandlingsansvarlige muligheten til å sikre at de samme plikter for behandling av personopplysninger pålegges underdatabehandleren. Bestemmelser for kommersielle forhold som ikke har betydning for behandling av personopplysninger under underdatabehandleravtalen, er ikke omfattet plikten til oversendelse til den behandlingsansvarlige.

6. Databehandleren skal avtale med underdatabehandleren at – i tilfelle konkurs hos databehandleren – den behandlingsansvarlige skal ha rettigheter som tredjepart under underdatabehandleravtalen og skal kunne håndheve rettigheter overfor underdata-

behandleren som engasjert av databehandleren, som f.eks. å gi den behandlingsansvarlige rett til å instruere underdatabehandleren til å slette eller tilbakelevere personopplysningene.

7. Dersom underdatabehandleren ikke oppfyller sine forpliktelser for databehandling, skal databehandleren overfor den behandlingsansvarlige ha fullt ansvar for at underdata-behandler oppfyller sine forpliktelser. Dette har ikke betydning for de rettigheter den registrerte har under GDPR – spesielt de rettigheter som er forutsatt i artikkel 79 og 82 i GDPR – overfor den behandlingsansvarlige og databehandleren, inkludert underdatabehandleren.

8 Overføring av personopplysninger til tredjestater eller internasjonale organisasjoner

1. Enhver overføring av personopplysninger til tredjestat eller internasjonale organisasjoner av databehandleren skal kun finne sted på grunnlag av dokumenterte instrukser fra den behandlingsansvarlige og skal kun skje i overensstemmelse med kapittel V i GDPR.

2. Dersom overføring til tredjestat eller internasjonale organisasjoner, som databehandleren ikke er blitt instruert til å foreta av den behandlingsansvarlige, som er påkrevet etter unionsretten eller Medlemsstatenes nasjonale rett som databehandleren er underlagt, skal databehandleren underrette den behandlingsansvarlige om nevnte rettslige krav før behandlingen, med mindre de rettslige kravene av hensyn til viktige allmenne interesser forbyr en slik underretning.

3. Uten dokumenterte instrukser fra den behandlingsansvarlige, kan databehandleren derfor ikke innenfor disse Kontrakts bestemmelser:

    a. Overføre personopplysninger til en behandlingsansvarlig eller databehandler i en tredjestat eller en internasjonal organisasjon

    b. overføre behandlingen av personopplysninger til en underdatabehandler i en tredjestat

    c. la personopplysningene behandles av en databehandler i en tredjestat

4. Den behandlingsansvarliges instrukser som gjelder overføring av personopplysninger til en tredjestat inkludert, hvis relevant, overføringsgrunnlagene etter kapittel V i GDPR som de er basert på, skal inntas i Vedlegg C.6.

5. Kontraktbestemmelsene skal ikke forstås som standard personvernbestemmelser etter artikkel 46(2)(c) og (d) i GDPR, og Kontrakts bestemmelsene kan benyttes som grunnlag som overføringsgrunnlag etter kapittel V i GDPR.

9 Bistand til den behandlingsansvarlige

1. Hensyntatt arten av behandling, databehandleren skal bistå den behandlingsansvarlige ved hjelp av egnede tekniske og organisatoriske tiltak, 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 kapittel III i GDPR.

Dette omfatter at databehandleren skal, i den grad det er mulig, bistå den behandlingsansvarlige i den behandlingsansvarliges overholdelse av:

a. Retten til å bli informert ved innsamling av personopplysninger fra den registrerte
b. retten til å bli informert dersom personopplysninger ikke har blitt samlet inn fra den registrerte
c. retten til innsyn av den registrerte
d. retten til retting
e. retten til sletting («retten til å bli glemt»)
f. retten til begrensning av behandling
g. underretningsplikt i forbindelse med retting eller sletting av personopplysninger eller begrensning av behandling
h. retten til dataportabilitet
i. retten til å protestere mot å omfattes av automatiserte individuelle avgjørelser, inkludert profilering.

2. Behandlingsansvarlig skal dekke kostnader knyttet til revisjoner som er initiert av Behandlingsansvarlig eller som påløper ved revisjon av Behandlingsansvarlig, inkludert kompensasjon til Databehandler for rimelig medgått tid.

3. I tillegg til databehandlerens plikt til å bistå den behandlingsansvarlige i henhold til punkt 6.4., databehandleren skal videre, hensyntatt arten av behandlingen og informasjon som er tilgjengelig for databehandleren, bistå den behandlingsansvarlige med overholdelse av:

   a. Den behandlingsansvarliges plikt uten ugrunnet opphold og når det er mulig, senest 72 timer etter å ha fått kjennskap til det, melde brudd på personopplysningssikkerheten til vedkommende tilsynsmyndighet, Datatilsynet, med mindre bruddet sannsynligvis ikke vil medføre en risiko for fysiske personers rettigheter og friheter,

   b. den behandlingsansvarliges plikt til å underrette om brudd på personopplysningssikkerheten til den registrerte, om det er sannsynlig at bruddet på personopplysningssikkerheten vil medføre en høy risiko for fysiske personers rettigheter og friheter,

   c. den behandlingsansvarliges plikt til å foreta en vurdering av hvilke konsekvenser den planlagte behandlingen vil ha for personopplysningsvernet (en vurdering av personvernkonsekvenser),

   d. den behandlingsansvarliges plikt til å rådføre seg med vedkommende tilsyns-myndighet, Datatilsynet, før behandling hvor en vurdering av personvern-konsekvensene som tilsier at behandlingen vil medføre en høy risiko dersom den behandlingsansvarlige ikke treffer tiltak for å redusere risikoen.

4. Partene skal angi i Vedlegg C egnede tekniske og organisatoriske tiltak som databehandleren skal bistå den behandlingsansvarlige med i tillegg til omfang og om bistand er påkrevet. Dette gjelder de plikter som er forutsatt i punkt 9.1. og 9.3.

10 Melding om brudd på personopplysningssikkerheten

1. I tilfelle brudd på personopplysningssikkerheten, skal databehandleren uten ugrunnet opphold etter å ha fått kjennskap til det, underrette den behandlingsansvarlige om bruddet på personopplysningssikkerheten.
2. Databehandlerens underretning til den behandlingsansvarlige skal, om mulig, skje innen 72 timer etter databehandleren har fått kjennskap til bruddet på personopplysnings-sikkerheten for å overholde den behandlingsansvarliges plikt til å melde bruddet på personopplysningssikkerheten til relevant tilsynsmyndighet, jf. artikkel 33 i GDPR.
3. I henhold til punkt 9(2)(a), databehandleren skal bistå den behandlingsansvarlige i å melde bruddet på personopplysningssikkerheten til vedkommende tilsynsmyndighet, hvilket omfatter at databehandleren skal bistå i å innhente informasjonen nedenfor som, i henhold til artikkel 33(3) i GDPR, skal inntas i den behandlingsansvarliges melding til vedkommende tilsynsmyndighet:
    a. Arten av personopplysninger, herunder når det er mulig, kategoriene av og omtrentlig antall registrerte som er berørt, og kategoriene av og omtrentlig antall registreringer av personopplysninger som er berørt,
    b. de sannsynlige konsekvensene av bruddet på personopplysningssikkerheten,
    c. de tiltak som er truffet eller foreslått å bli tatt av den behandlingsansvarlige for å håndtere bruddet på personopplysningssikkerheten, herunder, dersom det er relevant, tiltak for å redusere eventuelle skadevirkninger.
4. Partene skal angi i Vedlegg D det databehandleren skal tilveiebringe når denne bistår den behandlingsansvarlige i meldingen av bruddet på personopplysningssikkerheten til tilsynsmyndigheten.
5. Dersom avviket skyldes forhold på den behandlingsansvarliges side skal alle kostnader for databehandler dekkes av den behandlingsansvarlige.

11 Sletting og retur av data

1. Ved opphør av bestemmelsene om tjenestene knyttet til behandling av personopplysninger, er databehandleren forpliktet til å slette alle personopplysninger som er behandlet på vegne av den behandlingsansvarlige og bekrefte overfor den behandlingsansvarlige at dette er gjort.
2. Dersom behandlingsansvarlige ber om det plikter databehandler ved avtalens utløp å utlevere alle data som tilhører dem. Data vil være tilgjengelig i back-up i inntil 90 dager etter inaktivering for “gammelt” HMS-system. Dersom slik forespørsel kommer etter at slettingen i punkt 1 er gjennomført og datautleveringen medfører kostnader for databehandler skal disse dekkes av behandlingsansvarlig.
3. Databehandleren påtar seg å kun behandle personopplysninger for det formål og for den varighet som pålegges etter nevnte bestemmelser og kun under de betingelser som bestemmelsene setter.

12 Revisjon og inspeksjoner

1. Databehandleren skal gjøre tilgjengelig for den behandlingsansvarlige all informasjon som er nødvendig for å påvise overholdelse av pliktene som følger av artikkel 28 og Kontraktbestemmelsene, og tillate og bidra til revisjoner, inkludert inspeksjoner, utført av den behandlingsansvarlige eller annen revisor bemyndiget av den behandlingsansvarlige.
2. Fremgangsmåter for den behandlingsansvarliges revisjoner, inkludert inspeksjoner, av databehandleren og underdatabehandlere er regulert nærmere i Vedlegg C.7 and C.8.
3. Databehandleren skal være pålagt å gi tilsynsmyndigheter, som etter relevant lovgivning skal ha tilgang til den behandlingsansvarliges og databehandlers lokaler, eller representanter som handler på vegne av slike tilsynsmyndigheter, tilgang til databehandlerens fysiske lokaler ved fremleggelse av egnet identifikasjon.

13 Ytterligere bestemmelser

Partene kan avtale ytterligere bestemmelser vedrørende behandling av personopplysninger som spesifiserer f.eks. ansvar, så lenge disse ikke er i direkte eller indirekte motstrid med Kontraktbestemmelsene eller forringer de grunnleggende rettigheter og friheter for registrerte og den beskyttelse som GDPR gir.

14 Start og opphør

1. Kontraktbestemmelsene skal gjelde fra de er signert av begge parter.
2. Begge parter skal ha rett til å kreve at Kontraktbestemmelsene reforhandles dersom det skjer endringer i rettslige forhold eller uventede forhold gir grunn til slik reforhandling.
3. Kontraktbestemmelsene skal gjelde for så lenge det leveres tjenester knyttet til behandling av personopplysninger fra databehandleren. Så lenge det leveres tjenester for behandling av personopplysninger kan ikke Kontraktbestemmelsene sies opp dersom ikke andre bestemmelser om behandling av personopplysninger er avtalt mellom partene.
4. Dersom bestemmelser om behandling av personopplysninger sies opp, og person-opplysningene slettes eller tilbakeleveres til den behandlingsansvarlige etter punkt 11.1. og Vedlegg C.4, kan Kontrakts bestemmelsene sies opp med skriftlig varsel fra en av partene til den andre part.
5. Signatur

For databehandleren

Navn: Grønn Jobb AS

Stilling: Daglig leder

.....

Databehandler
Grønn Jobb AS
Dan Mario Røian, daglig leder

15 Den behandlingsansvarliges og databehandlers kontaktopplysninger

1. Partene kan kontakte hverandre ved følgende kontakter/kontaktpunkter:
2. Partene skal være forpliktet til å fortløpende informere hverandre om endringer i kontakter/kontaktpunkter.

For databehandleren

Grønn Jobb AS

post@gronnjobb.no

69 79 11 30

Vedlegg A Information om behandlingen

A.1. Formålet med databehandlerens behandling av personopplysninger på vegne av behandlingsansvarlig:

1. Formålet med databehandlers behandling av personopplysninger i HMS systemet er å sette behandlingsansvarlig i stand til å gjennomføre systematisk HMS arbeid digitalt. Modulen har også en app hvor HMS-avvik kan lagres direkte i systemet gjennom denne. Appen har funksjonalitet for å laste opp filer fra mobiltelefonen, for eksempel bilde av nevnte avvik.

3. Kursportalen har som formål å gjøre behandlingsansvarlig i stand til å gi de registrerte godkjent opplæring innen HMS og påfølgende kursbevis, digitalt gjennom systemet. Denne modulen har også en mobilapplikasjon som gir tilgang til den samme funksjonaliteten på app.

2. BHT-portalen har som formål å gjøre behandlingsansvarlig i stand til å hente ut dokumenter digitalt gjennom systemet. Denne modulen har også en mobilapplikasjon som gir tilgang til den samme funksjonaliteten på app.

4. HR-modulen har som formål å gjøre behandlingsansvarlig i stand til å gi de registrerte verktøy for å håndtere diverse HR oppgaver, som blant annet Timer, Ferie og Fravær. Denne modulen har også en mobilapplikasjon som gir tilgang til den samme funksjonaliteten på app.

5. Kurs-modulen har som formål å gjøre behandlingsansvarlig i stand til å gi de registrerte godkjent opplæring innen HMS og påfølgende kursbevis, digitalt gjennom systemet. Denne modulen har også en mobilapplikasjon som gir tilgang til den samme funksjonaliteten på app.

3. Behandling av personopplysninger i modulen prosjektstyringssystem har til hensikt å sette behandlingsansvarlig i stand til å styre prosjekter i henhold til regler og rutiner for bygg -og anleggsbransjen. Denne modulen har også en mobilapplikasjon som gjør det lettere for behandlingsansvarlig å føre kontroll på mobilen.

4. Støttemodulen Timeregistrering har som formål å hjelpe behandlingsansvarlig med å føre kontroll over medgått arbeidstid og utførte arbeidstimer digitalt. Modulen har også en app på mobiltelefon som gjør de registrerte i stand til å registrere timer enklere direkte gjennom appen.

5. Behandlingen av personopplysninger i støttemodulen for registrering av sykefravær lagrer aktive sykefravær og setter behandlingsansvarlig i stand til å behandle fraværet etter gjeldende regler. Mobilappen for sykefravær gjør det enklere for de registrerte å legge inn sykefraværet sitt direkte gjennom appen.

6. Modulen for IK-mat system benytter personopplysninger fra de registrerte for å levere en kontroll, avvik og varslingssystem for håndtering av mat i henhold til reglene for matsikkerhet.

6. Som en del av vår forpliktelse til å ivareta journalplikt, behandler BHT-tjenester personopplysninger i samsvar med lov om helsepersonell kapittel 8. Dette omfatter blant annet føring av nødvendige

helsejournaler for å gi forsvarlig helsehjelp. Videre oppfyller vi vårt rapporteringsansvar i henhold til Arbeidsmiljølovens § 3-3 og Forskrift om organisering, ledelse og medvirkning § 13-3, ved å behandle og rapportere relevante helse- og sikkerhetsopplysninger for å bidra til et trygt og sunt arbeidsmiljø.

7. Grønn Jobb kan lagre andre relevante data om de registrerte hos behandlingsansvarlig dersom den ansvarlige ber om bistand til for eksempel tilsynsrapporter fra Arbeidstilsynet, eller dersom de har andre utfordringer de trenger konsulær bistand til. Formålet vil i slike tilfeller være å løse situasjoner som ikke har vært i samsvar med loven eller å forhindre at slik situasjon skal oppstå.

A.2. Databehandlerens behandling av personopplysninger på vegne av den behandlingsansvarlige skal i hovedsak relatere seg til (behandlingens gjenstand):

- HMS systemet, med tilhørende støttemoduler
- HR systemet

8. Kursportal og BHT-portal
9. Søknadsprosesser til sentrale myndigheter

- Tilsynssaker og annen konsulær bistand

A.3. Behandlingen omfatter de følgende typer personopplysninger om de registrerte:

- Fullt navn
- Personnummer
- Bilde
- E-post adresse
- Firma adresse
- Organisasjonsnummer
- Telefonnummer/mobilnummer
- Stilling
- Fødselsdato / personnummer
- Postnummer og poststed
- Pårørende navn, relasjon og telefonnummer

Systemet lagrer i utgangspunktet ingen opplysninger som regnes som sensitive etter artikkel 9 og 10, men systemet har fritekstfelter der behandlingsansvarlig selv er ansvarlig for å ikke legge inn sensitive opplysninger. Unntaket er bedriftshelsetjenester hvor det vil kunne forekomme lagring av sensitive opplysninger i form av

helseopplysninger. Opplysningene vil lagres for å ivareta journalplikt i henhold til lov om helsepersonell kap 8, bedriftshelsetjenestens rapporteringsansvar i henhold til aml § 3-3 og Forskrift om organisering, ledelse og medvirkning § 13-3.

10. Notater fra enkeltkonsultasjoner
11. Notater fra arbeidsplassvurderinger
12. Helseundersøkelser
13. Konsultasjoner fra sykepleier, lege, fysioterapeut etc

A.4. Behandlingen omfatter følgende kategorier registrerte:

Alle ansatte og ledere som har avtale om kjøp eller bruk av systemer og tjenester fra Grønn Jobb As

A.5. Databehandlerens behandling av personopplysninger på vegne av behandlingsansvarlig kan utføres når Kontraktbestemmelsene får virkning. Behandlingen har følgende varighet:

Avtalen gjelder så lenge databehandler behandler personopplysninger på vegne av behandlingsansvarlig.

Ved opphør av avtalen slettes behandlingsansvarliges data og backup automatisk etter 90 dager fra og med tidspunktet der denne blir satt som" Inaktiv".

Vedlegg B Godkjente underdatabehandlere

B.1. Godkjente underdatabehandlere

Ved inngåelse av Kontraktbestemmelsene, gir den behandlingsansvarlige tillatelse til engasjement av følgende underdatabehandlere:

NAVN	ORG. NR.	ADRESSE	BESKRIVELSE AV BEHANDLINGEN
Back IT Up AS	997 864 913	Nedre Utgård 31, 1684 Vesterøy	Eier og drift av server systemet kjører på. Alle behandlinger fra punkt 1-6 i vedlegg A.1
Microsoft Norge AS (Skylagring)	957 485 030	Dronning Eufemias gate 71, 0194 Oslo	Lagring av opplysninger og kundedata knyttet til punkt 7-8 i vedlegg A1.
HubSpot		25 First Street, 2nd Floor Cambridge, MA 02141 United States	CRM system for lagring av kundedata. Brukes hovedsakelig med inbound marketing.
Extensor	987 403 594	Storgata 60, 8006 Bodø	Lagring av helseopplysninger i forbindelse med BHT-tjenester
Existec	984 489 234	Nye Vakåsvei 64, 1395 Hvalstad	ERP med fakturering mot alle kunder.
Survey Monkey		San Mateo, California, USA	Skybasert programvare for undersøkelser. Brukes for å utvikle og forbedre våre produkter basert på brukernes ønsker. Knyttet til punkt A.4

Den behandlingsansvarlige skal ved inngåelse av Kontraktbestemmelsene gi tillatelse til bruk av de ovennevnte underdatabehandlere for behandlingen beskrevet for denne. Databehandleren skal ikke ha rett til – uten den behandlingsansvarliges eksplisitte skriftlige tillatelse – å engasjere en underdatabehandler for «annen» behandling enn den som er blitt avtalt eller benytte en annen underdatabehandler til å foreta den beskrevne behandlingen.

Vedlegg C Instrukser for bruk av personopplysninger

C.1. Omfanget av/instrukser for behandlingen

Databehandlerens behandling av personopplysninger på vegne av behandlingsansvarlig skal bli utført av databehandleren på følgende måte:

Databehandleren skal gjennom sitt system utføre automatiske handlinger med å lagre, sammenstille, strukturere og dele personopplysninger innenfor rammene av systemet, slik at behandlingsansvarlig kan oppfylle de formålene som modulene er laget for og som er nevnt i vedlegg A.

Dette foregår ved at behandlingsansvarlig selv legger inn personopplysninger i systemets brukergrensesnitt og utfører handlinger ved hjelp av innebygde funksjoner. Selve lagringen og behandlingen av opplysningene foregår i databaser og lagrer opplysningene på en server hos tredjepart (se vedlegg B).

Databehandler kan også utføre manuell behandling av dataene på kundens forespørsel ved oppsett eller opplæring i systemets funksjoner. Ved feilrapporteringer eller når kunden ber om bistand kan databehandler be om tilgang og deretter gjøre de nødvendige tester og endringer for å løse problemet.

Databehandler er også instruert om å utlevere og eller slette opplysninger på kundens oppfordring, hvis kunden sier opp avtalen eller dersom behandlingsansvarlig misligholder avtalene for kjøp og bruk av tjenestene.

Databehandler skal ha kopi(backup) av alle produksjonsdata tilhørende kunde for å oppfylle kravet til tilstrekkelig sikkerhet for nevnte data. Disse kopiene skal også slettes i henhold til de til enhver tid gjeldende vilkår for sletting i hovedavtalen for databehandling.

Behandlinger som gjøres utenfor systemet for å bistå med søknader til renholdgodkjenning og sentralgodkjenning innebærer innsamling, lagring, sammenstilling og sending av data til statlige tredjeparter (Arbeidstilsynet) som også er behandlingsansvarlige for disse opplysningene.

Andre behandlinger utenfor systemet omfatter konsulær bistand ved for eksempel tilsynsrapporter. Her lagres informasjon som fremkommer i rapportene og andre data som kommer frem gjennom undersøkelsene som blir utført. Type og kategorier av personopplysninger går ikke utenfor det som allerede er nevnt og listet opp i denne avtalen. Selve behandlingen er lagring og sammenstilling av nevnte informasjon for å utbedre de feil som danner grunnlaget for tilsyn.

C.2. Sikkerhet ved behandlingen

Sikkerhetsnivået skal ta hensyn til:

At systemet lagrer omfattende mengder informasjon om norske og utenlandske arbeidstagere i Norge som registreres i systemet som kan påvirke folks liv og helse på arbeidsplassen. Opplysninger fra systemet kan også settes sammen til profiler som kan ha betydning for de registrertes rettigheter og friheter. Sikkerhetsnivået skal derfor ta hensyn til dette.

Databehandleren skal heretter ha rett til å ta beslutninger om tekniske og organisatoriske sikkerhetstiltak som skal iverksettes for å sørge for det nødvendige (og avtalte) sikkerhetsnivå.

Databehandleren skal allikevel – i alle tilfelle og minimum – implementere de følgende tiltak som er avtalt med den behandlingsansvarlige:

Hos Grønn Jobb har vi høyt fokus på sikkerhet. Vi har blant annet:

1. Sikkerhet i databaser
2. Innebygget i programvaren
3. På serveren
4. På nettverk knyttet til systemer og programvare
5. Fysiske sikkerhetstiltak
6. Proaktiv monitorering
7. Tilgangskontroll til fysiske lokasjoner, systemet, servere og database

Hosting og driftsleverandør (HMS-system tom 2022)

Grønn Jobb As bruker Back IT Up As som sin driftspartner. Data er lagret i Norge.

Servicen disse leverer inkluderer følgende tiltak for sikkerhet:

- Leie av server og utstyr
- Vedlikehold av maskinvare og oppgradering av BIOS/Firmware
- Monitorering av skylagring og programvare
- Oppdatering av antivirus programvare
- Kopi(backup) av alle kunde og virksomhetsdata.

Hosting og driftsleverandør (SaaS løsninger fom 2022)

Alle Grønn Jobb As sine nye SaaS produkter (fom 2022) bruker Microsoft Norge (Azure) som sin driftspartner. Data er lagret i Norge.

Servicen disse leverer inkluderer følgende tiltak for sikkerhet:

- Leie av server og utstyr
- Vedlikehold av maskinvare og oppgradering av BIOS/Firmware
- Monitorering av skylagring og programvare
- Oppdatering av antivirus programvare
- Kopi(backup) av alle kunde og virksomhetsdata.

Hosting og driftsleverandør (HMS-system fom 2022)

Grønn Jobb As bruker Microsoft Norge (Azure) som sin driftspartner. Data er lagret i Norge.

Servicen disse leverer inkluderer følgende tiltak for sikkerhet:

- Leie av server og utstyr
- Vedlikehold av maskinvare og oppgradering av BIOS/Firmware
- Monitorering av skylagring og programvare
- Oppdatering av antivirus programvare
- Kopi(backup) av alle kunde og virksomhetsdata.

Kryptering (SaaS løsninger fom 2022)

Alle personopplysninger relatert til systemet og som eksisterer i databasen er kryptert med krypteringsnøkkel som tilfredsstiller kravene fra datatilsynet.

All kommunikasjon og kryptering som flyter over nettet er kryptert med SSL (https). Mer om disse sertifikatene kan du se under.

Backup (BackIt Up)

Driftspartner kjører backup en gang i døgnet for alle kundedata og sender dette til hemmelig lokasjon. Grønn jobb kan gjenopprette og spore data fra kundedatabasen, dersom kunden ønsker det.

Begrensninger for backup: Vi kan ikke gjenspore eller tilbakekalle data fra kunder som har vært inaktive i mer enn 90 dager. Etter 90 dager slettes også alle backup filer i tråd med databehandleravtalen og vilkårene for personvern.

Backup etter 30 dager krever også en del manuelt arbeid og vil derfor ha en kostnad. Denne kostnaden må i slike tilfeller dekkes av kunden/den behandlingsansvarlige.

Tekniske og organisatoriske sikkerhetstiltak

- At tilgang til lokalene sikres med kodebrikke og kode.
- Tilgangskontroll med passordbeskyttelse på nettverk og godkjent brannmur.
- Tilgangskontroll med individuelle passord/kode på alle maskiner og fagsystemer
- Rutiner for bruk og oppbevaring av passord
- Overvåkning og monitorering av routertrafikk for å oppdage potensielle avvik og trusler
- Intern opplæring i IT sikkerhet og personvern

- Ekstern serverlokasjon og backup
- Krypteringsfunksjon på alle printere
- Kryptert tilkobling gjennom VPN for tilganger utenfor kontorlokalene

Backup (Microsoft Norge - Azure)

Microsoft kjører backup en gang i døgnet for alle kundedata som blir lagret i Norge. Grønn jobb kan gjenopprette og spore data fra kundedatabasen, dersom kunden ønsker det.

Se Microsoft Norge sine backup rutiner. Bakcup vil kun være mulig å hente ut 7 dager tilbake i tid. Backup vil da bli gjenopprettet for alle kunder.

Begrensninger for backup: Vi kan ikke gjenspore eller tilbakekalle data fra kunder som har vært inaktive i mer enn 90 dager. Etter 90 dager slettes også alle backup filer i tråd med databehandleravtalen og vilkårene for personvern.

C.3. Bistand til den behandlingsansvarlige

Databehandleren skal såfremt det er mulig – innenfor omfanget og i den grad bistanden er spesifisert nedenfor – bistå den behandlingsansvarlige i henhold til punkt 9.1 and 9.2 ved å implementere de følgende tekniske og organisatoriske tiltak:

9.1a) og b) Informasjonskravet til de registrerte er behandlingsansvarliges ansvar og kan gis på bakgrunn av informasjon som fremkommer i databehandleravtalen med vedlegg.

9.1.c) Retten opprettholdes av brukerens tilgang til systemet som gis av databehandler på instruks fra behandlingsansvarlig.

9.1.d) Retten til retting ivaretas av brukeren selv gjennom muligheten til å endre egen profilinformasjon som systemet kobler opp mot andre handlinger.

9.1.e) Retten til sletting må oppfylles av behandlingsansvarlig og databehandler gjør kun dette på instruks fra kunden eller dersom avtalen opphører. Dette gjøres manuelt og rutinebasert ved inaktivering av kunder. Selve sletterutinen på server blir startet av inaktiveringen og gjøres så automatisk.

9.1.f) og g) Disse pliktene er behandlingsansvarliges ansvar og påvirker ikke databehandler direkte. Dersom databehandler får slike instrukser vil det være rammene av systemet som bestemmer om dette er mulig. Dersom dette ikke er mulig, må kunden si opp systemet eller selv stoppe behandlingen innenfor rammene systemet har.

9.1.h) Dataportabilitet er oppfylt ved at alle funksjoner som sammenstiller og presenterer data i systemet er utskriftsbare. Loven krever dataene utlevert i et utskriftsvennlig format noe som tilbys gjennom de innebygde funksjonene i systemet.

9.1.i) Systemet utfører ikke automatiserte profileringer.

C.4. Fremgangsmåte for lagringstid/sletting

Personopplysninger skal lagres så lenge kundeforholdet og avtalen som regulerer dette er aktivt, hvoretter personopplysninger skal automatisk slettes av databehandleren.

Ved oppsigelse av bestemmelser om tjenester knyttet til behandlingen av personopplysninger, skal databehandleren enten slette eller tilbakelevere personopplysninger i henhold til punkt 11.1, hvis ikke den behandlingsansvarlige – etter inngåelse av avtalen – har endret den behandlingsansvarliges opprinnelige valg. Slik endring skal dokumenteres og oppbevares skriftlig, herunder elektronisk, i tilknytning til Kontraktbestemmelsene.

C.5. Behandlingssted

Behandling av personopplysninger etter Kontraktbestemmelsene skal ikke utføres på andre lokasjoner enn de følgende uten at det foreligger skriftlig forhåndssamtykke fra den behandlingsansvarlige:

- Backit Up: Hjalmar Bjørges vei 105, 1604 Fredrikstad - Norge

8. Grønn Jobb AS: Dikeveien 45, 1661 Rolvsøy - Norge

- Exitec: Nye Vakås vei 64, 1395 Hvalstad - Norge
- Microsoft Norge , Dronning Eufemias gate 71, 0194 Oslo

9. Hubspot: USA (AWS og GCP i Frankfurt 'EU')

- Visma, Norway
- Survey Monkey: USA / Irland

10. Extensor: På servere i regi av BackIt Up. Hjalmar Bjørges vei 105, 1604 Fredrikstad – Norge

C.6. Fremgangsmåte for den behandlingsansvarliges revisjoner, inkludert inspeksjoner, av behandlingen av personopplysninger som utføres av databehandleren

Databehandleren skal så lenge databehandleravtalen er gjeldende for behandlingsansvarliges kostnad innhente inspeksjonsrapporter fra en uavhengig tredjepart vedrørende databehandlerens overholdelse av GDPR, de relevante personvernreglene i unionsretten eller Medlemsstatenes nasjonale rett og Kontraktbestemmelsene.

Inspeksjonsrapportene skal uten ugrunnet opphold overendes den behandlingsansvarlige for informasjon. Den behandlingsansvarlige kan bestride omfanget og/eller metodikken for rapporten og kan i slikt tilfelle anmode om ny revisjon/inspeksjon med endret omfang og/eller annen metodikk.

Basert på resultatene av en slik revisjon/inspeksjon, den behandlingsansvarlige kan be om ytterligere tiltak for å sikre overholdelse av GDPR, de relevante personvernreglene i unionsretten eller Medlemsstatenes nasjonale rett og Kontraktbestemmelsene.

Den behandlingsansvarlig eller den behandlingsansvarliges representanter skal i tillegg ha tilgang til å inspisere, herunder fysisk inspisere, lokasjonene hvor behandlingen av personopplysninger gjennomføres av databehandleren, inkludert fysiske lokaler samt systemer benyttet for og knyttet til behandlingen. Slik inspeksjon skal bli utført når den behandlingsansvarlige anser det påkrevet.

Den behandlingsansvarliges kostnader, hvis aktuelt, knyttet til fysisk inspeksjon skal dekkes av den behandlingsansvarlige. Databehandleren skal imidlertid, være forpliktet til å bistå med ressurser (hovedsakelig tid) påkrevet for den behandlingsansvarlige til å gjennomføre inspeksjonen.