**Databehandlaravtale**

**(Standard kontraktsbestemmingar)**

*Etter artikkel 28(3) i forordning 2016/679 (GDPR)
(som basert på Opinion 14/2019 av Personvernrådet).*

Mellom

[NAMN]
Org. nr.: [ORG.NR.]
[ADRESSE]
[POSTNR. OG KOMMUNE]
[LAND]

(behandlingsansvarleg)

og

[NAMN]
Org. nr.: [ORG.NR.]
[ADRESSE]
[POSTNR. OG KOMMUNE]
[LAND]

(databehandlar)

kvar omtalt som ein «part», eller saman som «partane»,

har avtalt dei følgjande standard kontraktsbestemmingane (Kontraktsbestemmingane) for å oppfylle krava i GDPR og for vern av den registrerte sine rettar.

# Innhald

[1 Innhald 1](#_Toc38608292)

[2 Innleiing 2](#_Toc38608293)

[3 Behandlingsansvarleges rettar og plikter 3](#_Toc38608294)

[4 Databehandlaren skal handle etter instruksar 3](#_Toc38608295)

[5 Konfidensialitet 3](#_Toc38608296)

[6 Sikkerheit ved behandlinga 4](#_Toc38608297)

[7 Bruk av underdatabehandlarar 4](#_Toc38608298)

[8 Overføring av personopplysingar til tredje statar eller internasjonale organisasjonar 6](#_Toc38608299)

[9 Bistand til den behandlingsansvarlege 6](#_Toc38608300)

[10 Melding om brot på personopplysingssikkerheita 7](#_Toc38608301)

[11 Sletting og retur av data 8](#_Toc38608302)

[12 Revisjon og inspeksjonar 8](#_Toc38608303)

[13 Ytterlegare bestemmingar 8](#_Toc38608304)

[14 Start og opphøyr 9](#_Toc38608305)

[15 Den behandlingsansvarleges og databehandlars kontaktopplysingar 9](#_Toc38608306)

[Vedlegg A Information om behandlinga 11](#_Toc38608307)

[Vedlegg B Godkjente underdatabehandlarar 12](#_Toc38608308)

[Vedlegg C Instruksar for bruk av personopplysingar 13](#_Toc38608309)

[Vedlegg D ytterlegare bestemmingar avtalt mellom partane 18](#_Toc38608310)

# Innleiing

1. Desse standard kontraktsbestemmingane (Kontraktsbestemmingane) regulerer rettar og plikter for behandlingsansvarleg og databehandlar, når det behandlast personopplysingar på vegner av den behandlingsansvarlege.
2. Kontraktsbestemmingane er utforma for å sikre at partane overheld artikkel 28 (3) i Europaparlaments- og rådsforordning (EU) 2016/679 av 27. april 2016 om vern av fysiske personar i samband med behandling av personopplysingar og om fri utveksling av slike opplysingar, samt om oppheving av direktiv 95/46/EF (generell personvernforordning - GDPR).
3. I samband med leveranse av [NAMN PÅ TENESTER], vil databehandlaren behandle personopplysingar på vegner av den behandlingsansvarlege i medhald av Kontraktsbestemmingane.
4. Kontraktsbestemmingane skal ha forrang over andre tilsvarande bestemmingar i andre avtalar mellom partane.
5. Fire vedlegg er inntatt i Kontraktsbestemmingane og vert rekna som omfatta av Kontraktsbestemmingane.
6. Vedlegg A inneheldt detaljar om behandlinga av personopplysingar, medrekna behandlingas formål og art, typen personopplysingar, kategoriar av registrerte og varigheita av behandlinga.
7. Vedlegg B inneheldt vilkåra til den behandlingsansvarlege for databehandlarens bruk av underdatabehandlarar og ei liste over underdatabehandlarar godkjent av den behandlingsansvarlege.
8. Vedlegg C inneheldt instruksjonane til den behandlingsansvarlege for behandlinga av personopplysingar, minimum sikkerheitstiltak som skal implementerast av databehandlaren og korleis revisjonar av databehandlaren og eventuelle underdatabehandlarar skal gjennomførast.
9. Vedlegg D inneheldt regulering av andre aktivitetar som ikkje er dekka av Kontraktsbestemmingane.
10. Kontraktsbestemmingane saman med vedlegga skal takast imot skriftleg, inkludert elektronisk, av begge partar.
11. Kontraktsbestemmingane skal ikkje frita databehandlaren frå plikter som databehandlaren skal følgje etter personvernforordninga (GDPR) eller anna lovgiving.

# Rettar og plikter til behandlingsansvarlege

1. Den behandlingsansvarlege er ansvarleg for å sikre at behandlinga av personopplysingar utførast i samsvar med GDPR (sjå artikkel 24 i GDPR), personvernreglane i gjeldande EU eller Medlemsstats[[1]](#footnote-2) personvernreglar og Kontraktsbestemmingane.
2. Den behandlingsansvarlege har rett og plikt til å fatte slutningar om formåla med og midlane for behandlinga av personopplysingar.
3. Den behandlingsansvarlege skal vere ansvarleg for å sikre at behandlinga av personopplysingar, som databehandlaren er instruert om å utføre, har eit rettsleg grunnlag.

# Databehandlaren skal handle etter instruksar

1. Databehandlaren skal berre behandle personopplysingar på dokumenterte instruksar frå den behandlingsansvarlege, med mindre det krevst i samband med unionsretten eller den nasjonale retten til Medlemsstatane som databehandlaren er underlagt. Slike instruksar skal vere spesifisert i vedlegg A og C. Seinare instruksar kan også bli gjeven av den behandlingsansvarlege under behandlinga av personopplysingar, men slike instruksar skal alltid vere dokumenterte og oppbevarast i skriftleg form, for eksempel elektronisk, i overeinskomst med Kontraktsbestemmingane.
2. Databehandlaren skal omgåande underrette den behandlingsansvarlege dersom vedkommande meiner at ein instruks gjeven av den behandlingsansvarlege er i strid med GDPR eller andre slutningar om vern av personopplysingar i unionsretten eller den nasjonale retten til Medlemsstatane.

[MERK: PARTANE SKAL VURDERE KONSEKVENSAR SOM KAN OPPSTÅ AV EVENTUELLE INSTRUKSJONAR SOM IKKJE ER I TRÅD MED LOVVERKET, SOM ER GJEVEN AV DEN BEHANDLINGSANSVARLEGE, OG REGULERE DETTE I AVTALEN MELLOM PARTANE.]

# Konfidensialitet

1. Databehandlaren skal berre gje tilgang til personopplysingar som behandlast på vegner av den behandlingsansvarlege til personar som er under databehandlarens myndigheit og som er forplikta til konfidensialitet eller er underlagt eigna lovfesta teieplikt og som kun har nødvendig behov for tilgang. Lista over personar som har tilgang til personopplysingane skal regelmessig bli gjennomgått. Som følgje av gjennomgangen skal tilgang til personopplysingane bli trekt tilbake dersom slik tilgang ikkje lenger er nødvendig for personane.
2. Databehandlaren skal på oppmoding frå den behandlingsansvarlege vise at dei involverte personane under databehandlarens myndigheit er omfatta av ovannemnde konfidensialitetsplikt.

# Sikkerheit ved behandlinga

1. Artikkel 32 i GDPR angjev at, idet det vert tatt omsyn til den tekniske utviklinga, gjennomføringskostnadane og behandlingas art, omfang, formål av behandlinga og samanhengen den vert utført i, samt risikoane av varierande sannsyns- og alvorsgrad for fysiske personars retter og fridom, skal den behandlingsansvarlege og databehandlaren gjennomføre eigna tekniske og organisatoriske tiltak for å oppnå eit sikkerheitsnivå som er eigna med omsyn til risikoen.

Den behandlingsansvarlege skal vurdere risikoen til rettar og fridom for fysiske personar som omfattast av behandlinga og implementere tiltak for å redusere risikoen. Avhengig av relevans, kan tiltaka omfatte følgjande:

* 1. Pseudonymisering og kryptering av personopplysingar,
	2. evne til å sikre vedvarande konfidensialitet, integritet, tilgang og vere robust i behandlingssystema og -tenestene,
	3. evne til å rette opp att tilgangen og tilgangen til personopplysingar i rett tid dersom det oppstår ei fysisk eller teknisk hending,
	4. ein prosess for regelmessig testing, analysering og vurdering av kor effektive behandlinga si tekniske og organisatoriske sikkerheitstiltak er.
1. I samsvar med artikkel 32 i GDPR, skal databehandlaren også – uavhengig frå den behandlingsansvarlege – vurdere risikoen til rettar og fridom for fysiske personar som omfattast av behandlinga og implementere tiltak for å redusere risikoen. For dette formål skal den behandlingsansvarlege gje databehandlaren all informasjon som er nødvendig for å identifisere og vurdere slik risiko.
2. Videre skal databehandlaren hjelpe den behandlingsansvarlege i å sikre at pliktane til den behandlingsansvarlege vert overheldt etter artikkel 32 i GDPR, ved å m.a. sørge for at den behandlingsansvarlege får informasjon om tekniske og organisatoriske tiltak som er implementert av databehandlaren i samsvar med artikkel 32 i GDPR, saman med all anna informasjon som er nødvendig for den behandlingsansvarlege til å overhalde plikter under artikkel 32 i GDPR.

Dersom det i ettertid – etter vurdering av den behandlingsansvarlege – viser seg at reduksjon av den identifiserte risiko krev implementering av ytterlegare tiltak av databehandlaren enn dei tiltak som allereie er implementert av databehandlaren etter artikkel 32 i GDPR, skal den behandlingsansvarlege spesifisere desse ytterlegare tiltaka som skal implementerast i Vedlegg C.

# Bruk av underdatabehandlarar

1. Databehandlaren skal overhalde krava i artikkel 28(2) og (4) i GDPR for å engasjere ein anna databehandlar (ein underdatabehandlar).
2. Databehandlaren skal difor ikkje engasjere anna databehandlar (underdatabehandlar) for oppfylling av Kontraktsbestemmingane utan at det på førehand er innhenta [ALTERNATIV 1] særleg skriftleg tillating / [ALTERNATIV 2] generell skriftleg tillating frå den behandlingsansvarlege.
3. [ALTERNATIV 1 SÆRLEG SKRIFTLEG TILLATING] Databehandlaren skal engasjere underdatabehandlarar kun dersom det finst særleg skriftleg tillating frå den behandlingsansvarlege. Databehandlaren skal spørje om særleg tillating minst [SPESIFISER TIDSPERIODE] før den aktuelle underdatabehandlaren skal engasjerast. Liste over under­databehandlarar som allereie er godkjent av den behandlingsansvarlege kan takast inn i Vedlegg B.

[ALTERNATIV 2 GENERELL SKRIFTLEG TILLATING] Databehandlaren er gjeven generell tillating frå den behandlingsansvarlege for å engasjere underdatabehandlarar. Databehandlaren skal skriftleg underrette den behandlingsansvarlege om eventuelle planar om å nytte andre underdatabehandlarar eller skifte ut underdatabehandlarar minst [SPESIFISER TIDSPERIODE] på førehand, og dermed gje den behandlingsansvarlege moglegheita til å motsetje seg slike endringar før underdatabehandlar(ar) engasjerast. Ytterlegare tid for å underrette for spesifikk underdatabehandling kan bli teken inn i Vedlegg B. Liste over under­databehandlarar som allereie er godkjent av den behandlingsansvarlege kan takast inn i Vedlegg B.

1. Dersom databehandlaren engasjerer ein underdatabehandlar for å utføre spesifikke behandlings­aktivitetar på vegner av den behandlingsansvarlege, skal dei same forpliktingane som er fastsett i Kontraktsbestemmingane bli pålagt underdatabehandlaren ved avtale eller eit annet rettsleg dokument i samsvar med unionsretten eller den nasjonale retten til Medlemsstatane, der det særleg vert gjeven tilstrekkelege garantiar for at det vil bli gjennomført tekniske og organisatoriske tiltak som sikrar at behandlinga oppfyller krava i Kontraktsbestemmingane og GDPR.

Databehandlaren skal difor vere ansvarleg for at under­data­behandlaren minimum overheldt dei forpliktingar som databehandlaren er pålagt etter Kontraktsbestemmingane og GDPR.

1. Ein kopi av slik underdatabehandlaravtale og etterfølgjande endringar skal – på den behandlingsansvarleges oppmoding – sendast over den behandlingsansvarlege, og dermed gje den behandlingsansvarlege moglegheita til å sikre at dei same plikter for behandling av person­opplysingar påleggjast underdatabehandlaren. Bestemmingar for kommersielle forhold som ikkje har betyding for behandling av personopplysingar under underdata­behandlar­avtalen, er ikkje omfatta plikten til oversending til den behandlingsansvarlege.
2. Databehandlaren skal avtale med underdatabehandlaren at – i tilfelle konkurs hos databehandlaren – den behandlingsansvarlege skal ha rettar som tredjepart under under­databehandlar­avtalen og skal kunne handheve rettar overfor under­data­behandlaren som er engasjert av databehandlaren, som f.eks. å gje den behandlingsansvarlege rett til å instruere underdatabehandlaren til å slette eller levere tilbake personopplysingane.
3. Dersom underdatabehandlaren ikkje oppfyller sine forpliktingar for databehandling, skal databehandlaren overfor den behandlingsansvarlege ha fullt ansvar for at under­data­behandlar oppfyller sine forpliktingar. Dette har ikkje betyding for dei rettar den registrerte har under GDPR – spesielt dei rettar som er forutsett i artikkel 79 og 82 i GDPR – ovanfor den behandlingsansvarlege og databehandlaren, inkludert underdatabehandlaren.

# Overføring av personopplysingar til tredje statar eller internasjonale organisasjonar

1. Ei overføring av personopplysingar til ein tredje stat eller internasjonale organisasjonar av databehandlaren skal kun finne stad på grunnlag av dokumenterte instruksar frå den behandlingsansvarlege og skal kun skje i samsvar med kapittel V i GDPR.
2. Dersom overføring til tredje stat eller internasjonale organisasjonar, som databehandlaren ikkje er blitt instruert til å foreta av den behandlingsansvarlege, som er kravd etter unionsretten eller den nasjonale retten til Medlemsstatane som databehandlaren er underlagt, skal databehandlaren underrette den behandlingsansvarlege om nemnde rettslege krav før behandlinga, med mindre dei rettslege krava av omsyn til viktige allmenne interesser forbyr ein slik informasjon.
3. Utan dokumenterte instruksar frå den behandlingsansvarlege, kan databehandlaren difor ikkje innanfor desse Kontraktsbestemmingar:
	1. Overføre personopplysingar til ein behandlingsansvarleg eller databehandlar i ein tredje stat eller ein internasjonal organisasjon
	2. overføre behandlinga av personopplysingar til ein underdatabehandlar i ein tredje stat
	3. la personopplysingane behandlast av ein databehandlar i ein tredje stat
4. Instruksar kring overføring av personopplysingar frå den behandlingsansvarlege til ein tredje stat inkludert, dersom relevant, grunnlaga for overføring etter kapittel V i GDPR som dei er basert på, skal bli teken inn i Vedlegg C.6.
5. Kontraktsbestemmingane skal ikkje bli forstått som standard personvernbestemmingar etter artikkel 46(2)(c) og (d) i GDPR, og Kontraktsbestemmingane kan nyttast som grunnlag for overføring etter kapittel V i GDPR.

# Bistand til den behandlingsansvarlege

1. Arten av behandling skal takast omsyn til, og databehandlaren skal hjelpe den behandlingsansvarlege ved hjelp av eigna tekniske og organisatoriske tiltak, i den grad det er mogleg, med å oppfylle plikta til den behandlingsansvarlege til å svare på oppmodingar som den registrerte gjev med hensikt for å utøve sine rettar fastsett i kapittel III i GDPR.

Dette omfattar at databehandlaren skal, i den grad det er mogleg, bistå den behandlingsansvarlege å overhalde:

* 1. Retten til å bli informert ved innsamling av personopplysingar frå den registrerte
	2. retten til å bli informert dersom personopplysingar ikkje har blitt samla inn frå den registrerte
	3. retten til innsyn av den registrerte
	4. retten til retting
	5. retten til sletting («retten til å bli gløymt»)
	6. retten til avgrensing av behandling
	7. informasjonsplikt i samband med retting eller sletting av personopplysingar eller avgrensing av behandling
	8. retten til dataportabilitet
	9. retten til å protestere mot å omfattast av automatiserte individuelle avgjersler, inkludert profilering
1. I tillegg til databehandlaren sin plikt til å bistå den behandlingsansvarlege i samsvar med punkt 6.3., skal databehandlaren videre ta omsyn til arten av behandlinga og informasjon som er tilgjengeleg for databehandlaren, og bistå den behandlingsansvarlege med å overhalde:
	1. Den behandlingsansvarlege si plikt utan ugrunna opphald og når det er mogleg, seinast 72 timar etter å ha fått kjennskap til det, melde brot på personopplysings­sikkerheita til vedkomande tilsynsmyndigheit, Datatilsynet, med mindre brotet sannsynlegvis ikkje vil medføre ein risiko for fysiske personars rettar og fridom,
	2. den behandlingsansvarlege si plikt til å underrette om brot på personopplysings­sikkerheita til den registrerte, om det er sannsynleg at brotet på person­opplysings­sikkerheita vil medføre ein høy risiko for fysiske personars rettar og fridom,
	3. den behandlingsansvarlege si plikt til å foreta ei vurdering av kva konsekvensar den planlagde behandlinga vil ha for personopplysingsvernet (ei vurdering av personvern­konsekvensar),
	4. den behandlingsansvarlege si plikt til å rådføre seg med vedkomande tilsyns­myndigheit, Datatilsynet, før behandling der ei vurdering av personvern­konsekvensane som tilseier at behandlinga vil medføre ein høy risiko dersom den behandlingsansvarlege ikkje treffer tiltak for å redusere risikoen.
2. Partane skal angje i Vedlegg C eigna tekniske og organisatoriske tiltak som databehandlaren skal bistå den behandlingsansvarlege med, i tillegg til omfang og om bistand er kravd. Dette gjelder dei plikter som er forutsett i punkt 9.1. og 9.2.

# Melding om brot på personopplysingssikkerheita

1. I tilfelle brot på personopplysingssikkerheita, skal databehandlaren utan ugrunna opphald etter å ha fått kjennskap til det, underrette den behandlingsansvarlege om brotet på personopplysingssikkerheita.
2. Databehandlarens informasjon til den behandlingsansvarlege skal, om mogleg, skje innan [TAL PÅ TIMAR] etter databehandlaren har fått kjennskap til brotet på person­opplysings­sikkerheita for å overhalde den behandlingsansvarlege si plikt til å melde brotet på personopplysingssikkerheita til relevant tilsynsmyndigheit, jf. artikkel 33 i GDPR.
3. I samsvar med punkt 9(2)(a), databehandlaren skal bistå den behandlingsansvarlege i å melde brotet på personopplysingssikkerheita til vedkomande tilsynsmyndigheit, noko som omfattar at databehandlaren skal bistå i å innhente informasjonen nedanfor som, i samsvar med artikkel 33(3) i GDPR, skal bli teken inn i den behandlingsansvarlege si melding til vedkomande tilsynsmyndigheit:
	1. Arten av personopplysingar, for eksempel når det er mogleg, kategoriane av og omtrentleg tal på registrerte som er rørt, og kategoriane av og omtrentleg tal på registreringar av personopplysingar som er rørt,
	2. dei sannsynlege konsekvensane av brotet på personopplysingssikkerheita,
	3. dei tiltak som er treft eller føreslått å bli tatt av den behandlingsansvarlege for å handtere brotet på personopplysingssikkerheita, for eksempel, dersom det er relevant, tiltak for å redusere eventuelle skadeverknader.
4. Partane skal angje i Vedlegg D det databehandlaren skal finne fram når denne hjelper den behandlingsansvarlege i meldinga av brotet på personopplysingssikkerheita til tilsynsmyndigheitene.

# Sletting og retur av data

1. Ved opphøyr av bestemmingane om tenestene knytt til behandling av personopplysingar, er databehandlaren forplikta til [ALTERNATIV 1] å slette alle personopplysingar som er behandla på vegner av den behandlingsansvarlege og bekrefte overfor den behandlingsansvarlege at dette er gjort / [ALTERNATIV 2] levere tilbake alle personopplysingane til den behandlingsansvarlege og slette eksisterande kopiar, med mindre unionsretten eller den nasjonale retten til Medlemsstatane krev at personopplysingane vert lagra.
2. [ALTERNATIV] Følgjande bestemmingar i unionsretten eller den nasjonale retten til Medlemsstatane som omfattar databehandlaren pålegg lagring av personopplysingar etter opphøyr av bestemmingar om tenester knytt til behandlinga av personopplysingar:
	1. […]

Databehandlaren tek berre på seg å handsama personopplysingar for det formål og for den varigheit som påleggjast etter nemnde bestemmingar og berre under dei føresetnader som bestemmingane set.

# Revisjon og inspeksjonar

1. Databehandlaren gjer tilgjengeleg for den behandlingsansvarlege all informasjon som er nødvendig for å påvise overhalding av pliktene som følger av artikkel 28 og Kontraktsbestemmingane, og tillate og bidra til revisjonar, inkludert inspeksjonar, utført av den behandlingsansvarlege eller anna revisor gjort myndig av den behandlingsansvarlege.
2. Framgangsmåtar for den behandlingsansvarleges revisjonar, inkludert inspeksjonar, av databehandlaren og underdatabehandlarar er regulert nærare i Vedlegg C.7 og C.8.
3. Databehandlaren skal vere pålagt å gje tilsynsmyndigheiter, som etter relevant lovgiving skal ha tilgang til lokala til den behandlingsansvarlege og databehandlaren, eller representantar som handlar på vegner av slike tilsynsmyndigheiter, tilgang til databehandlarens fysiske lokale ved framlegging av eigna identifikasjon.

# Ytterlegare bestemmingar

Partane kan avtale ytterlegare bestemmingar kring behandling av personopplysingar som spesifiserer f.eks. ansvar, så lenge desse ikkje er direkte eller indirekte i strid med Kontraktsbestemmingane eller svekker dei grunnleggande rettane og fridomen for den registrerte og det vern som GDPR gjev.

# Start og opphøyr

1. Kontraktsbestemmingane skal gjelde når dei er signert av begge partar.
2. Begge partar skal ha rett til å krevje at Kontraktsbestemmingane reforhandlast dersom det skjer endringar i rettslege forhold eller uventa forhold gjev grunn til slik reforhandling.
3. Kontraktsbestemmingane skal gjelde for så lenge det vert levert tenester knytt til behandling av personopplysingar frå databehandlaren. Så lenge det vert levert tenester for behandling av personopplysingar kan ikkje Kontraktsbestemmingane seiast opp, dersom ikkje andre bestemmingar om behandling av personopplysingar er avtalt mellom partane.
4. Dersom bestemmingar om behandling av personopplysingar seiast opp, og person­opplysingane slettast eller vert levert tilbake til den behandlingsansvarlege etter punkt 11.1. og Vedlegg C.4, kan Kontraktsbestemmingane seiast opp med skriftleg varsel frå ein av partane til den andre parten.
5. Signatur

For den behandlingsansvarlege

Namn [NAMN]

Stilling [STILLING]

Dato [DATO]

Signatur [SIGNATUR]

For databehandlaren

Namn [NAMN]

Stilling [STILLING]

Dato [DATO]

Signatur [SIGNATUR]

# Kontaktopplysingar til den behandlingsansvarlege og databehandlaren

1. Partane kan kontakte kvarandre ved følgjande kontaktar/kontaktpunkt:
2. Partane skal vere forplikta til å fortlaupande informere kvarandre om endringar i kontaktar/kontaktpunkt.

For den behandlingsansvarlege

Namn [NAMN]

Stilling [STILLING]

Telefon [TELEFON]

E-post [E-POST]

For databehandlaren

Namn [NAMN]

Stilling [STILLING]

Telefon [TELEFON]

E-post [E-POST]

# Vedlegg A Informasjon om behandlinga

[MERK: DERSOM DET SKAL GJENNOMFØRAST FLEIRE BEHANDLINGSAKTIVITETAR, MÅ PUNKTA NEDANFOR FYLLAST UT FOR Å DEKKJE KVAR AV BEHANDLINGSAKTIVITETANE.]

## A.1. Formålet med databehandlaren sin behandling av personopplysingar på vegner av den behandlingsansvarleg:

[BESKRIV FORMÅLET MED BEHANDLINGA].

## A.2. Databehandlaren sin behandling av personopplysingar på vegner av den behandlingsansvarlege skal i hovudsak relatere seg til (behandlingas gjenstand):

[BESKRIV GJENSTANDEN FOR BEHANDLINGA].

## A.3. Behandlinga omfattar dei følgjande typar personopplysingar om dei registrerte:

[BESKRIV TYPEN PERSONOPPLYSINGAR SOM SKAL BEHANDLAST – FOR EKSEMPEL:]

“Namn, e-postadresse, telefonnummer, adresse, fødselsnummer, betalingsinformasjon, medlemsnummer, type medlemskap, deltaking på treningssenter og påmelding på spesifikke treningstimar.”

[MERK: BESKRIVINGA BØR GJERAST PÅ MEST MOGLEG DETALJERT MÅTE, OG UNDER EINKVAR OMSTENDE, TYPANE PERSONOPPLYSINGAR MÅ VERE SPESIFISERT I STØRRE GRAD ENN KUN VISING TIL «PERSONOPPLYSINGAR SOM ANGJEVEN I ARTIKKEL 4(1) AV GDPR» ELLER ANGJE KVA KATEGORIAR («ARTIKKEL 6, 9 OG 10 I GDPR») AV PERSONOPPLYSINGAR SOM ER GJENSTAND FOR BEHANDLINGA.]

## A.4. Behandlinga omfattar følgjande kategoriar registrerte:

[SKRIV INN KATEGORIAR AV REGISTRERTE].

## A.5. Databehandlarens behandling av personopplysingar på vegner av behandlingsansvarleg kan utførast når Kontraktsbestemmingane får verknad. Behandlinga har følgjande varigheit:

[SKRIV INN VARIGHEITA AV BEHANDLINGA].

# Vedlegg B Godkjente underdatabehandlarar

## B.1. Godkjente underdatabehandlarar

Ved inngåing av Kontraktsbestemmingane, gjev den behandlingsansvarlege tillating til engasjement av følgjande underdatabehandlarar:

|  |  |  |  |
| --- | --- | --- | --- |
| **NAMN** | **ORG. NR.** | **ADRESSE** | **BESKRIVING AV BEHANDLINGA** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Den behandlingsansvarlege skal ved inngåing av Kontraktsbestemmingane gje tillating til bruk av dei ovannemnde underdatabehandlarar for behandlinga beskriven for denne. Databehandlaren skal ikkje ha rett til – utan den behandlingsansvarlege si eksplisitte skriftlege tillating – å engasjere ein underdatabehandlar for «anna» behandling enn den som er avtalt eller nytte ein annan underdatabehandlar til å gjere den beskrivne behandlinga.

## B.2. Føregåande varsel for tillating til underdatabehandlarar

[ALTERNATIV] [DERSOM RELEVANT, BESKRIV TIDSPERIODEN FOR FØREGÅANDE VARSEL FOR TILLATING TIL BRUK AV UNDERDATABEHANDLARAR]

# Vedlegg C Instruksar for bruk av personopplysingar

## C.1. Omfanget av/instruksar for behandlinga

Databehandlarens behandling av personopplysingar på vegner av behandlingsansvarleg skal bli utført av databehandlaren på følgjande måte:

[BESKRIV BEHANDLINGA SOM DATABEHANDLAREN ER BLITT INSTRUERT TIL Å GJENNOMFØRE].

## C.2. Sikkerheit ved behandlinga

Sikkerheitsnivået skal ta omsyn til:

[OMSYNTATT ART, OMFANG, SAMANHENG OG FORMÅL AV BEHANDLINGSAKTIVITETEN, SAMT RISIKOANE AV VARIERANDE SANNSYN- OG ALVORSGRAD FOR FYSISKE PERSONARS RETTAR OG FRIDOM, BESKRIV FORHOLD SOM HAR BETYDING FOR SIKKERHEITSNIVÅET, FOR EKSEMPEL:]

*«At behandlinga omfattar eit stort omfang av personopplysingar som omfattast av artikkel 9 i GDPR om ‘særlege kategoriar personopplysingar’ som er årsaka til at eit ‘høgare’ nivå av sikkerheit bør etablerast.»*

Databehandlaren skal heretter ha rett til å gjera slutningar om tekniske og organisatoriske sikkerheitstiltak som skal setjast i verk for å syte for det nødvendige (og avtalte) sikkerheitsnivå.

Databehandlaren skal likevel – i alle tilfelle og som eit minimum – implementere dei følgjande tiltak som er avtalt med den behandlingsansvarlege:

[BESKRIV KRAVA FOR PSEUDONYMISERING OG KRYPTERING AV PERSONOPPLYSINGAR]

[BESKRIV KRAVA FOR Å SIKRE KONFIDENSIALITET, INTEGRITET, TILGANG OG Å VERE ROBUST I BEHANDLINGSSYSTEMA OG -TENESTER]

[BESKRIV KRAVA TIL Å GJENOPPRETTE TILGANG TIL PERSONOPPLYSINGAR I TILFELLE EI FYSISK ELLER TEKNISK HENDING]

[BESKRIV KRAVA FOR BEHANDLING FOR REGELMESSIG TESTING, TILGANG OG EVALUERING AV EFFEKTIVITETEN AV TEKNISKE OG ORGANISATORISKE TILTAK FOR Å SIKRE SIKKERHEITA VED BEHANDLINGA]

[BESKRIV KRAVA FOR TILGANG TIL DATA ONLINE]

[BESKRIV KRAVA FOR VERN AV DATA VED OVERFØRING]

[BESKRIV KRAVA FOR VERN AV DATA VED LAGRING]

[BESKRIV KRAVA FOR FYSISK SIKKERHEIT VED LOKALITETAR DER PERSONOPPLYSINGAR VERT BEHANDLA]

[BESKRIV KRAVA FOR HEIMEARBEID/FJERNTILGANG]

[BESKRIV KRAVA FOR LOGGFØRING]

## C.3. Bistand til den behandlingsansvarlege

Databehandlaren skal soframt det er mogleg – innanfor omfanget og i den grad bistanden er spesifisert nedanfor – bistå den behandlingsansvarlege i samsvar med punkt 9.1 and 9.2 ved å implementere dei følgjande tekniske og organisatoriske tiltak:

[BESKRIV OMFANGET OG DEN GRAD AV ASSISTANSE SOM SKAL YTAST AV DATABEHANDLAREN]

[BESKRIV DEI SPESIFIKKE TEKNISKE OG ORGANISATORISKE TILTAK SOM SKAL TAKAST AV DATABEHANDLAREN FOR Å YTE BISTAND TIL DEN BEHANDLINGSANSVARLEGE]

## C.4. Framgangsmåte for lagringstid/sletting

[TA INN LAGRINGSPERIODE/FRAMGANGSMÅTE FOR SLETTING FOR DATABEHANDLAREN, DERSOM AKTUELT FOR EKSEMPEL:]

Personopplysingar skal vert lagra [TA INN TIDSPERIODE ELLER HENDING] og deretter skal personopplysingar automatisk slettast av databehandlaren.

Ved oppseiing av bestemmingar om tenester knytt til behandlinga av personopplysingar, skal databehandlaren anten slette eller levere tilbake personopplysingar i samsvar med punkt 11.1, dersom ikkje den behandlingsansvarlege – etter inngåing av avtalen – har endra den behandlingsansvarlege sitt opphavelege val. Ei slik endring skal dokumenterast og oppbevarast skriftleg, for eksempel elektronisk, i tilknyting til Kontraktsbestemmingane.

## C.5. Behandlingsstad

Behandling av personopplysingar etter Kontraktsbestemmingane skal ikkje utførast på andre lokalitetar enn dei følgjande, utan at det finst skriftleg førehandssamtykke frå den behandlingsansvarlege:

[ANGJE KVAR BEHANDLINGA SKAL SKJE]

[ANGJE DATABEHANDLAREN ELLER UNDERDATABEHANDLARAR MED ADRESSE]

## C.6. Instruksar for overføring av personopplysingar til ein tredje stat

[BESKRIV INSTRUKSAR FOR OVERFØRING AV PERSONOPPLYSINGAR TIL EIN TREDJE STAT ELLER INTERNASJONAL ORGANISASJON]

[ANGJE DET RETTSLEGE GRUNNLAG FOR OVERFØRING ETTER KAPITTEL V I GDPR]

Dersom den behandlingsansvarlege verken i Kontraktsbestemmingane eller i det etterfølgjande gjev dokumenterte instruksar kring overføring av personopplysingar til ein tredje stat, skal databehandlaren ikkje ha rett til å overføre personopplysingar til ein tredje stat innanfor rammene av Kontraktsbestemmingane.

## C.7. Framgangsmåte for den behandlingsansvarlege sine revisjonar, inkludert inspeksjonar, av behandlinga av personopplysingar som utførast av databehandlaren

[BESKRIV FRAMGANGSMÅTEN FOR BEHANDLINGSANSVARLEGES REVISJONAR, INKLUDERT INSPEKSJONAR, AV BEHANDLINGA FOR PERSONOPPLYSINGAR AV DATABEHANDLAREN – FOR EKSEMPEL]

Databehandlaren skal [TA INN TIDSPERIODE] for [DATABEHANDLAREN SIN/­BEHANDLINGSANSVARLEGE SINE] kostnad innhente [REVISORRAPPORTAR/INSPEKSJONSRAPPORTAR] frå ein uavhengig tredjepart kring databehandlaren sin overhalding av GDPR, dei relevante personvernreglane i unionsretten eller den nasjonale retten til Medlemsstatane og Kontraktsbestemmingane.

Partane har avtalt at dei følgjande typar [REVISORRAPPORTAR/INSPEKSJONSRAPPORTAR] kan nyttast for overhalding av Kontraktsbestemmingane:

[TA INN «GODKJENTE» REVISORRAPPORTAR/INSPEKSJONSRAPPORTAR]

[REVISORRAPPORTANE/INSPEKSJONSRAPPORTANE] skal utan ugrunna opphald oversendast den behandlingsansvarlege for informasjon. Den behandlingsansvarlege kan stride imot omfanget og/eller metodikken for rapporten og kan i slike tilfelle oppmoda om ny revisjon/inspeksjon med endra omfang og/eller anna metodikk.

Basert på resultata av ein slik revisjon/inspeksjon, kan den behandlingsansvarlege be om ytterlegare tiltak for å sikre at GDPR vert overhalden, dei relevante personvernreglane i unionsretten eller den nasjonale retten til Medlemsstatane og Kontraktsbestemmingane.

Den behandlingsansvarleg eller den behandlingsansvarlege sine representantar skal i tillegg ha tilgang til å inspisere, for eksempel fysisk inspisere, lokalitetane der behandlinga av personopplysingar vert gjennomført av databehandlaren, inkludert fysiske lokale, samt systema nytta for og knytt til behandlinga. Slik inspeksjon skal bli utført når den behandlingsansvarlege ser dette kravd.

[ELLER]

Den behandlingsansvarlege eller den behandlingsansvarlege sine representantar skal [TA INN TIDSPERIODE] utføre fysisk inspeksjon av lokalitetar der behandlinga av personopplysingar vert gjennomført av databehandlaren, inkludert fysiske lokale samt systema nytta for og knytt til behandlinga for å sikre databehandlaren sin overhalding av GDPR, dei relevante personvernreglane i unionsretten eller den nasjonale retten til Medlemsstatane og Kontraktsbestemmingane.

I tillegg til dei planlagde inspeksjonar, kan den behandlingsansvarleg utføre inspeksjonar av databehandlaren når den behandlingsansvarlege ser dette kravd.

[OG DERSOM RELEVANT]

Den behandlingsansvarlege sine kostnadar, dersom aktuelt, knytt til fysisk inspeksjon skal dekkjast av den behandlingsansvarlege. Databehandlaren skal samstundes vere forplikta til å hjelpa med ressursar (hovudsakleg tid) kravd for den behandlingsansvarlege til å gjennomføre inspeksjonen.

## C.8. [DERSOM RELEVANT] Framgangsmåtar for revisjonar, inkludert inspeksjonar, av behandlinga av personopplysingar som utførast av underdatabehandlarar

[DERSOM RELEVANT, BESKRIV FRAMGANGSMÅTAR FOR BEHANDLINGSANSVARLEGE SINE REVISJONAR, INKLUDERT INSPEKSJONAR, FOR BEHANDLING AV PERSONOPPLYSINGAR SOM UTFØRAST AV UNDERDATABEHANDLAR – FOR EKSEMPEL]

Databehandlaren skal [TA INN TIDSPERIODE] for [DATABEHANDLAREN SIN­N/BEHANDLINGSANSVARLEGE SINE] kostand innhente [REVISORRAPPORTAR/INSPEKSJONSRAPPORTAR] frå ein uavhengig tredjepart kring underdatabehandlaren sin overhalding av GDPR, dei relevante personvernreglane i unionsretten eller den nasjonale retten til Medlemsstatane og Kontraktsbestemmingane.

Partane har avtalt at dei følgjande typar [REVISORRAPPORTAR/INSPEKSJONSRAPPORTAR] kan nyttast for overhalding av Kontraktsbestemmingane:

[TA INN «GODKJENTE» REVISORRAPPORTAR/INSPEKSJONSRAPPORTAR]

[REVISORRAPPORTANE/INSPEKSJONSRAPPORTANE] skal utan ugrunna opphald sendast over til den behandlingsansvarlege for informasjon. Den behandlingsansvarlege kan stride imot omfanget og/eller metodikken for rapporten og kan i slike tilfelle oppmoda om ny revisjon/inspeksjon med endra omfang og/eller anna metodikk.

Basert på resultata av ein slik revisjon/inspeksjon, kan den behandlingsansvarlege be om ytterlegare tiltak for å sikre overhalding av GDPR, dei relevante personvernreglane i unionsretten eller den nasjonale retten til Medlemsstatane og Kontraktsbestemmingane.

Den behandlingsansvarlege eller den behandlingsansvarlege sine representantar skal i tillegg ha tilgang til å inspisere, for eksempel fysisk inspisere, lokalitetane der behandlinga av personopplysingar vert gjennomført av underdatabehandlaren, inkludert fysiske lokale, samt systema nytta for og knytt til behandlinga. Slik inspeksjon skal bli utført når databehandlaren (eller den behandlingsansvarlege) ser dette kravd.

Dokumentasjon for slike inspeksjonar skal utan opphald sendast over til den behandlingsansvarlege for informasjon. Den behandlingsansvarlege kan stride imot omfanget og/eller metodikken for rapporten og kan i slike tilfelle oppmoda om ny inspeksjon med endra omfang og/eller anna metodikk.

[ELLER]

Databehandlaren eller databehandlarens representantar skal [TA INN TIDSPERIODE] utføre fysisk inspeksjon av lokalitetar der behandlinga av personopplysingar vert gjennomført av underdatabehandlaren, inkludert fysiske lokale, samt systema nytta for og knytt til behandlinga for å sikre at underdatabehandlaren overheldt GDPR, dei relevante personvernreglane i unionsretten eller den nasjonale retten til Medlemsstatane og Kontraktsbestemmingane.

I tillegg til dei planlagde inspeksjonar, kan databehandlaren utføre inspeksjonar av underdatabehandlaren når databehandlaren (eller den behandlingsansvarlege) ser dette kravd.

Dokumentasjon for slike inspeksjonar skal utan ugrunna opphald sendast over til den behandlingsansvarlege for informasjon. Den behandlingsansvarlege kan stride imot omfanget og/eller metodikken for rapporten og kan i slike tilfelle oppmoda om ny inspeksjon med endra omfang og/eller anna metodikk.

Basert på resultata av ein slik inspeksjon, kan den behandlingsansvarleg be om ytterlegare tiltak for å sikre at GDPR vert overhalden, dei relevante personvernreglane i unionsretten eller den nasjonale retten til Medlemsstatane og Kontraktsbestemmingane.

[OG DERSOM RELEVANT]

Den behandlingsansvarleg kan – dersom kravd – velje å initiere og delta i ein fysisk inspeksjon av underdatabehandlaren. Dette kan gjelde dersom den behandlingsansvarlege ser at databehandlaren sin kontroll av underdatabehandlaren ikkje har gjeven den behandlingsansvarlege tilstrekkeleg dokumentasjon til å vurdere om behandlinga av underdatabehandlaren vert utført i samsvar med Kontraktsbestemmingane.

Behandlingsansvarlege si deltaking i ein inspeksjon av underdatabehandlaren skal ikkje endre det forhold at databehandlaren har det fulle ansvar for underdatabehandlarens overhalding av GDPR, dei relevante personvernreglane i unionsretten eller den nasjonale retten til Medlemsstatane og Kontraktsbestemmingane.

[OG DERSOM RELEVANT]

Databehandlaren sin og underdatabehandlaren sine kostnader til fysiske kontroll/inspeksjon av underdatabehandlaren sine lokale skal ikkje belastast den behandlingsansvarlege – uavhengig av om den behandlingsansvarlege har initiert og deltatt i ein slik inspeksjon.

# Vedlegg D Ytterlegare bestemmingar avtalt mellom partane

1. Vising til “Medlemsstat” i Kontraktsbestemmingane skal verte forstått som vising til EØS-medlemsstatar. [↑](#footnote-ref-2)