**Databehandleravtale**

**(Standard kontraktsbestemmelser)**

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

Mellom

[NAVN]
Org. nr.: [ORG. NR.]
[ADRESSE]
[POST NR. OG KOMMUNE]
[LAND]

(behandlingsansvarlig)

og

[NAVN]
Org. nr.: [ORG. NR.]
[ADRESSE]
[POST NR. OG KOMMUNE]
[LAND]

(databehandler)

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

Har avtalt de følgende standard kontraktsbestemmelser (Kontraktsbestemmelsene) for å oppfylle kravene i GDPR og for vern av den registrertes rettigheter.

# Innhold

[1 Innhold 1](#_Toc33454641)

[2 Innledning 2](#_Toc33454642)

[3 Behandlingsansvarliges rettigheter og plikter 3](#_Toc33454643)

[4 Databehandleren skal handle etter instrukser 3](#_Toc33454644)

[5 Konfidensialitet 3](#_Toc33454645)

[6 Sikkerhet ved behandlingen 4](#_Toc33454646)

[7 Bruk av underdatabehandlere 4](#_Toc33454647)

[8 Overføring av personopplysninger til tredjestater eller internasjonale organisasjoner 6](#_Toc33454648)

[9 Bistand til den behandlingsansvarlige 6](#_Toc33454649)

[10 Melding om brudd på personopplysningssikkerheten 7](#_Toc33454650)

[11 Sletting og retur av data 8](#_Toc33454651)

[12 Revisjon og inspeksjoner 8](#_Toc33454652)

[13 Ytterligere bestemmelser 8](#_Toc33454653)

[14 Start og opphør 9](#_Toc33454654)

[15 Den behandlingsansvarliges og databehandlers kontaktopplysninger 9](#_Toc33454655)

[Vedlegg A Information om behandlingen 11](#_Toc33454656)

[Vedlegg B Godkjente underdatabehandlere 12](#_Toc33454657)

[Vedlegg C Instrukser for bruk av personopplysninger 13](#_Toc33454658)

[Vedlegg D Ytterligere bestemmelser avtalt mellom partene 18](#_Toc33454659)

# Innledning

1. Disse standard kontraktsbestemmelser (Kontraktsbestemmelsene) regulerer rettigheter og plikter for behandlingsansvarlig og databehandler, når det behandles personopplysninger på vegne av den behandlingsansvarlige.
2. Kontraktsbestemmelsene 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 [NAVN PÅ TJENESTER], vil databehandleren behandle personopplysninger på vegne av den behandlingsansvarlige i henhold til Kontraktsbestemmelsene.
4. Kontraktsbestemmelsene skal ha forrang over andre tilsvarende bestemmelser i andre avtaler mellom partene.
5. Fire vedlegg er inntatt i Kontraktsbestemmelsene og anses som omfattet av Kontraktsbestemmelsene.
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. Vedlegg D inneholder regulering av andre aktiviteter som ikke er dekket av Kontraktsbestemmelsene.
10. Kontraktsbestemmelsene sammen med vedleggene skal mottas skriftlig, inkludert elektronisk, av begge parter.
11. Kontraktsbestemmelsene skal ikke frita databehandleren fra plikter som databehandleren skal følge etter personvernforordningen (GDPR) eller annen lovgivning.

# 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]](#footnote-2) personvernregler og Kontraktsbestemmelsene.
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.

# 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 iløpet av behandlingen av personopplysninger, men slike instrukser skal alltid være dokumenterte og oppbevares i skriftlig form, herunder elektronisk, i overensstemmelse med Kontraktsbestemmelsene.
2. Databehandleren skal omgående underrette den behandlingsansvarlige dersom vedkommende mener at en instruks gitt av den behandlingsansvarlige er i strid med GDPR eller andre bestemmelser om vern av personopplysninger i unionsretten eller Medlemsstatenes nasjonale rett.

[MERK: PARTENE SKAL VURDERE KONSEKVENSER SOM KAN OPPSTÅ AV EVENTUELLE INSTRUKSJONER SOM IKKE ER I HENHOLD TIL LOVVERKET SOM ER GITT AV DEN BEHANDLINGSANSVARLIGE OG REGULERE DETTE I AVTALEN MELLOM PARTENE.]

# 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 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 til for personene.
2. Databehandleren skal på anmodning fra den behandlingsansvarlige påvise at de involverte personene under databehandlerens myndighet er omfattet av ovennevnte konfidensialitetsplikt.

# 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:

* 1. Pseudonymisering og kryptering av personopplysninger,
	2. evne til å sikre vedvarende konfidensialitet, integritet, tilgjengelighet og robusthet i behandlingssystemene og -tjenestene,
	3. evne til å gjenopprette tilgjengeligheten og tilgangen til personopplysninger i rett tid dersom det oppstår en fysisk eller teknisk hendelse,
	4. en prosess for regelmessig testing, analysering og vurdering av hvor effektive behandlingens tekniske og organisatoriske sikkerhetstiltak er.
1. 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 formal skal den behandlingsansvarlige tilveiebringe databehandleren med all informasjon som er nødvendig for å identifisere og vurdere slik risiko.
2. 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 det i ettertid – ved vurderingen foretatt av den behandlingsansvarlige – viser seg at 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.

# 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 Kontraktsbestemmelsene uten at det på forhånd er innhentet [ALTERNATIV 1] særlig skriftlig tillatelse / [ALTERNATIV 2] generell skriftlig tillatelse fra den behandlingsansvarlige.
3. [ALTERNATIV 1 SÆRLIG SKRIFTLIG TILLATELSE] Databehandleren skal engasjere underdatabehandlere kun dersom det foreligger særlig skriftlig tillatelse fra den behandlingsansvarlige. Databehandleren skal forespørre om særlig tillatelse minst [SPESIFISER TIDSPERIODE] før den aktuelle underdatabehandler skal engasjeres. Liste over under­databehandlere som allerede er godkjent av den behandlingsansvarlige kan inntas i Vedlegg B.

[ALTERNATIV 2 GENERELL SKRIFTLIG TILLATELSE] 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 [SPESIFISER TIDSPERIODE] 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.

1. Dersom databehandleren engasjerer en underdatabehandler for å utføre spesifikke behandlings­aktiviteter på vegne av den behandlingsansvarlige, skal de samme forpliktelsene som er fastsatt i Kontraktsbestemmelsene 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 Kontrakts­bestem­melsene og GDPR.

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

1. 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.
2. 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 under­data­behandleren som engasjert av databehandleren, som f.eks. å gi den behandlingsansvarlige rett til å instruere underdatabehandleren til å slette eller tilbakelevere personopplysningene.
3. Dersom underdatabehandleren ikke oppfyller sine forpliktelser for databehandling, skal databehandleren overfor den behandlingsansvarlige ha fullt ansvar for at under­data­behandler 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.

# 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 Kontraktsbestemmelser:
	1. Overføre personopplysninger til en behandlingsansvarlig eller databehandler i en tredjestat eller en internasjonal organisasjon
	2. overføre behandlingen av personopplysninger til en underdatabehandler i en tredjestat
	3. la personopplysningene behandles av en databehandler i en tredjestat
4. Den behandlingsansvarliges instrukser vedrørende 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. Kontraktsbestemmelsene skal ikke forstås som standard personvernbestemmelser etter artikkel 46(2)(c) og (d) i GDPR, og Kontraktsbestemmelsene kan ikke benyttes som overføringsgrunnlag etter kapittel V i GDPR.

# Bistand til den behandlingsansvarlige

1. Hensyntatt arten av behandling, skal databehandleren 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, i den grad det er mulig, skal bistå den behandlingsansvarlige med den behandlingsansvarliges overholdelse av:

* 1. Retten til å bli informert ved innsamling av personopplysninger fra den registrerte
	2. retten til å bli informert dersom personopplysninger ikke har blitt samlet inn fra den registrerte
	3. retten til innsyn av den registrerte
	4. retten til retting
	5. retten til sletting («retten til å bli glemt»)
	6. retten til begrensning av behandling
	7. underretningsplikt i forbindelse med retting eller sletting av personopplysninger eller begrensning av behandling
	8. retten til dataportabilitet
	9. retten til å protestere mot å omfattes av automatiserte individuelle avgjørelser, inkludert profilering
1. I tillegg til databehandlerens plikt til å bistå den behandlingsansvarlige i henhold til punkt 6.3., skal databehandleren videre, hensyntatt arten av behandlingen og informasjon som er tilgjengelig for databehandleren, bistå den behandlingsansvarlige med overholdelse av:
	1. Den behandlingsansvarliges plikt til 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,
	2. 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,
	3. den behandlingsansvarliges plikt til å foreta en vurdering av hvilke konsekvenser den planlagte behandlingen vil ha for personopplysningsvernet (en vurdering av personvern­konsekvenser),
	4. den behandlingsansvarliges plikt til å rådføre seg med vedkommende tilsyns­myndighet, Datatilsynet, før behandling hvor en vurdering av personvern­konsekvensene som tilsier at behandlingen vil medføre en høy risiko dersom den behandlings­ansvarlige ikke treffer tiltak for å redusere risikoen.
2. 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 9.2.

# 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 [ANTALL TIMER] timer etter databehandleren har fått kjennskap til bruddet på person­opplysnings­sikkerheten 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:
	1. 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,
	2. de sannsynlige konsekvensene av bruddet på personopplysningssikkerheten,
	3. 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.

# Sletting og retur av data

1. Ved opphør av bestemmelsene om tjenestene knyttet til behandling av personopplysninger, er databehandleren forpliktet til [ALTERNATIV 1] å slette alle personopplysninger som er behandlet på vegne av den behandlingsansvarlige og bekrefte overfor den behandlings­ansvarlige at dette er gjort / [ALTERNATIV 2] tilbakeleverer alle personopplysningene til den behandlingsansvarlige og sletter eksisterende kopier, med mindre unionsretten eller Medlemsstatenes nasjonale rett krever at personopplysningene lagres.
2. [ALTERNATIV] Følgende bestemmelser i unionsretten eller Medlemsstatenes nasjonale rett som omfatter databehandleren pålegger lagring av personopplysninger etter opphør av bestemmelser om tjenester knyttet til behandlingen av personopplysninger:
	1. […]

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.

# Revisjon og inspeksjoner

1. Databehandleren gjøre tilgjengelig for den behandlingsansvarlige all informasjon som er nødvendig for å påvise overholdelse av pliktene som følger av artikkel 28 og Kontraktsbestemmelsene, 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 og 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.

# 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 Kontraktsbestemmelsene eller forringer de grunnleggende rettigheter og friheter for registrerte og den beskyttelse som GDPR gir.

# Start og opphør

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

For den behandlingsansvarlige

Navn [NAVN]

Stilling [STILLING]

Dato [DATO]

Signatur [SIGNATUR]

For databehandleren

Navn [NAVN]

Stilling [STILLING]

Dato [DATO]

Signatur [SIGNATUR]

# 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 den behandlingsansvarlige

Navn [NAVN]

Stilling [STILLING]

Telefon [TELEFON]

E-post [E-POST]

For databehandleren

Navn [NAVN]

Stilling [STILLING]

Telefon [TELEFON]

E-post [E-POST]

# Vedlegg A Information om behandlingen

[MERK: DERSOM DET SKAL FORETAS FLERE BEHANDLINGSAKTIVITETER, PUNKTENE NEDENFOR MÅ FYLLES UT FOR Å DEKKE HVER AV BEHANDLINGSAKTIVITETENE.]

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

[BESKRIV FORMÅLET MED BEHANDLINGEN].

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

[BESKRIV GJENSTANDEN FOR BEHANDLINGEN].

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

[BESKRIV TYPEN PERSONOPPLYSNINGER SOM SKAL BEHANDLES – FOR EKSEMPEL:]

“Navn, e-postadresse, telefonnummer, adresse, fødselsnummer, betalingsinformasjon, medlemsnummer, type medlemskap, deltakelse på treningssenter og påmelding på spesifikke treningstimer.”

[MERK: BESKRIVELSEN BØR GJØRES PÅ MEST MULIG DETALJERT MÅTE, OG UNDER ENHVER OMSTENDIGHET, TYPENE PERSONOPPLYSNINGER MÅ VÆRE SPESIFISERT I STØRRE GRAD ENN KUN HENVISNING TIL «PERSONOPPLYSNINGER SOM ANGITT I ARTIKKEL 4(1) AV GDPR» ELLER ANGI HVILKE KATEGORIER («ARTIKKEL 6, 9 OG 10 I GDPR») AV PERSONOPPLYSNINGER SOM ER GJENSTAND FOR BEHANDLINGEN.]

## A.4. Behandlingen omfatter følgende kategorier registrerte:

[INNTA KATEGORIER AV REGISTRERTE].

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

[INNTA VARIGHETEN AV BEHANDLINGEN].

# Vedlegg B Godkjente underdatabehandlere

## B.1. Godkjente underdatabehandlere

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

|  |  |  |  |
| --- | --- | --- | --- |
| **NAVN** | **ORG. NR.** | **ADRESSE** | **BESKRIVELSE AV BEHANDLINGEN** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Den behandlingsansvarlige skal ved inngåelse av Kontraktsbestemmelsene 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.

## B.2. Forutgående varsel for tillatelse for underdatabehandlere

[ALTERNATIV] [HVIS RELEVANT, BESKRIV TIDSPERIODEN FOR FORUTGÅENDE VARSEL FOR TILLATELSE FOR BRUK AV UNDERDATABEHANDLERE]

# 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:

[BESKRIV BEHANDLINGEN SOM DATABEHANDLEREN ER BLITT INSTRUERT TIL Å GJENNOMFØRE].

## C.2. Sikkerhet ved behandlingen

Sikkerhetsnivået skal ta hensyn til:

[HENSYNTATT ART, OMFANG, SAMMENHENG OG FORMÅL AV BEHANDLINGSAKTIVITETEN, SAMT RISIKOENE AV VARIERENDE SANNSYNLIGHETS- OG ALVORLIGHETSGRAD FOR FYSISKE PERSONERS RETTIGHETER OG FRIHETER, BESKRIV FORHOLD SOM HAR BETYDNING FOR SIKKERHETSNIVÅET, FOR EKSEMPEL:]

«At behandlingen omfatter et stort omfang av personopplysninger som omfattes av artikkel 9 i GDPR om ‘særlige kategorier personopplysninger’ som er årsaken til et ‘høyere’ nivå av sikkerhet bør etableres.»

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:

[BESKRIV KRAVENE FOR:

* Pseudonymisering og kryptering av personopplysninger
* Å sikre konfidensialitet, integritet, tilgjengelighet og robusthet for behandlingssystemer og -tjenester
* Mulighetene til å gjenopprette tilgjengelighet og tilgang til personopplysninger rettidig i tilfelle en fysisk eller teknisk hendelse
* Behandling for regelmessig testing, tilgang og evaluering av effektiviteten av tekniske og organisatoriske tiltak for å sikre sikkerheten ved behandlingen
* Tilgang til data online
* Beskyttelse av data ved overføring
* Beskyttelse av data ved lagring
* Fysisk sikkerhet ved lokasjoner hvor personopplysninger blir behandlet
* Hjemmearbeid/fjerntilgang
* Loggføring]

## 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 og 9.2 ved å implementere de følgende tekniske og organisatoriske tiltak:

[BESKRIV OMFANGET OG DEN GRAD AV ASSISTANSE SOM SKAL YTES AV DATABEHANDLEREN]

[BESKRIV DE SPESIFIKKE TEKNISKE OG ORGANISATORISKE TILTAK SOM SKAL TAS AV DATABEHANDLEREN FOR Å YTE BISTAND TIL DEN BEHANDLINGSANSVARLIGE]

## C.4. Fremgangsmåte for lagringstid/sletting

[TA INN LAGRINGSPERIODE/FREMGANGSMÅTE FOR SLETTING FOR DATABEHANDLEREN, HVIS AKTUELT FOR EKSEMPEL:]

Personopplysninger skal lagres [TA INN TIDSPERIODE ELLER HENDELSE] hvoretter personopplysninger skal automatisk slettes av databehandleren.

Ved oppsigelse av bestemmelser om tjenester knyttet til behandlingen av personopplysninger, databehandleren skal 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 Kontraktsbestemmelsene.

## C.5. Behandlingssted

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

[ANGI HVOR BEHANDLINGEN SKAL SKJE]

[ANGI DATABEHANDLERENS ELLER UNDERDATABEHANDLERE MED ADRESSE]

## C.6. Instrukser for overføring av personopplysninger tredjestat

[BESKRIV INSTRUKSER FOR OVERFØRING AV PERSONOPPLYSNINGER TIL TREDJESTAT ELLER INTERNASJONAL ORGANISASJON]

[ANGI DET RETTSLIGE GRUNNLAG FOR OVERFØRING ETTER KAPITTEL V I GDPR]

Dersom den behandlingsansvarlige verken i Kontraktsbestemmelsene eller i det etterfølgende gir dokumenterte instrukser vedrørende overføring av personopplysninger til en tredjestat, skal databehandleren ikke ha rett til å overføre personopplysninger til tredjestat innenfor rammene av Kontraktsbestemmelsene.

## C.7. Fremgangsmåte for den behandlingsansvarliges revisjoner, inkludert inspeksjoner, av behandlingen av personopplysninger som utføres av databehandleren

[BESKRIV FREMGANGSMÅTEN FOR BEHANDLINGSANSVARLIGES REVISJONER, INKLUDERT INSPEKSJONER, AV BEHANDLINGEN FOR PERSONOPPLYSNINGER AV DATABEHANDLEREN – FOR EKSEMPEL]

Databehandleren skal [TA INN TIDSPERIODE] for [DATABEHANDLERENS/­BEHANDLINGS­ANSVARLIGES] kostnad innhente [REVISORRAPPORTER/INSPEKSJONSRAPPORTER] fra en uavhengig tredjepart vedrørende databehandlerens overholdelse av GDPR, de relevante personvernreglene i unionsretten eller Medlemsstatenes nasjonale rett og Kontraktsbestemmelsene.

Partene har avtalt at de følgende typer [REVISORRAPPORTER/INSPEKSJONSRAPPORTER] kan benyttes for overholdelse av Kontraktsbestemmelsene:

[TA INN «GODKJENTE» REVISORRAPPORTER/INSPEKSJONSRAPPORTER]

[REVISORRAPPORTENE/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 Kontraktsbestemmelsene.

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.

[ELLER]

Den behandlingsansvarlig eller den behandlingsansvarliges representanter skal [TA INN TIDSPERIODE] utføre fysisk inspeksjon av lokasjoner hvor behandlingen av personopplysninger gjennomføres av databehandleren, inkludert fysiske lokaler samt systemer benyttet for og knyttet til behandlingen for å sikre databehandlerens overholdelse av GDPR, de relevante personvernreglene i unionsretten eller Medlemsstatenes nasjonale rett og Kontraktsbestemmelsene.

I tillegg til de planlagte inspeksjoner, den behandlingsansvarlig kan utføre inspeksjoner av databehandleren når den behandlingsansvarlige anser det påkrevet.

[OG HVIS RELEVANT]

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.

## C.8. [HVIS RELEVANT] Fremgangsmåter for revisjoner, inkludert inspeksjoner, av behandlingen av personopplysninger som utføres av underdatabehandlere

[HVIS RELEVANT, BESKRIV FREMGANGSMÅTER FOR BEHANDLINGSANSVARLIGES REVISJONER, INKLUDERT INSPEKSJONER, AV BEHANDLING AV PERSONOPPLYSNINGER SOM UTFØRES AV UNDERDATABEHANDLER – FOR EKSEMPEL]

Databehandleren skal [TA INN TIDSPERIODE] for [DATABEHANDLERENS­/BEHANDLINGS­ANSVARLIGES] kostand innhente [REVISORRAPPORTER/INSPEKSJONSRAPPORTER] fra en uavhengig tredjepart vedrørende underdatabehandlerens overholdelse av GDPR, de relevante personvernreglene i unionsretten eller Medlemsstatenes nasjonale rett og Kontraktsbestemmelsene.

Partene har avtalt at de følgende typer [REVISORRAPPORTER/INSPEKSJONSRAPPORTER] kan benyttes for overholdelse av Kontraktsbestemmelsene:

[TA INN «GODKJENTE» REVISORRAPPORTER/INSPEKSJONSRAPPORTER]

[REVISORRAPPORTENE/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 Kontraktsbestemmelsene.

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

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

[ELLER]

Databehandleren eller databehandlerens representanter skal [TA INN TIDSPERIODE] utføre fysisk inspeksjon av lokasjoner hvor behandlingen av personopplysninger gjennomføres av underdatabehandleren, inkludert fysiske lokaler samt systemer benyttet for og knyttet til behandlingen for å sikre underdatabehandlerens overholdelse av GDPR, de relevante personvernreglene i unionsretten eller Medlemsstatenes nasjonale rett og Kontraktsbestemmelsene.

I tillegg til de planlagte inspeksjoner, databehandleren kan utføre inspeksjoner av underdatabehandleren når databehandleren (eller den behandlingsansvarlige) anser det påkrevet.

Dokumentasjon for slike inspeksjoner 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 inspeksjon med endret omfang og/eller annen metodikk.

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

[OG HVIS RELEVANT]

Den behandlingsansvarlig kan – hvis påkrevet – velge å initiere og delta i en fysisk inspeksjon av underdatabehandleren. Dette kan gjelde dersom den behandlingsansvarlige anser at databehandlerens kontroll av underdatabehandleren ikke har gitt den behandlingsansvarlige tilstrekkelig dokumentasjon til å vurdere om behandlingen av underdatabehandleren utføres i henhold til Kontraktsbestemmelsene.

Behandlingsansvarliges deltakelse i en inspeksjon av underdatabehandleren skal ikke endre det forhold at databehandleren har det fulle ansvar for underdatabehandlerens overholdelse av GDPR, de relevante personvernreglene i unionsretten eller Medlemsstatenes nasjonale rett og Kontraktsbestemmelsene.

[OG HVIS RELEVANT]

Databehandlerens og underdatabehandlerens kostnader til fysiske kontroll/inspeksjon av underdatabehandlerens lokaler skal ikke belastes den behandlingsansvarlige – uavhengig av om den behandlingsansvarlige har initiert og deltatt i slik inspeksjon.

# Vedlegg D Ytterligere bestemmelser avtalt mellom partene

1. Henvisning til “Medlemsstat” i Kontraktsbestemmelsene skal forstås som henvisning til EØS-medlemsstater. [↑](#footnote-ref-2)