Databehandleravtale

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

Mellom

Kunde:
Org. Nr:
Adresse:
(behandlingsansvarlig)

Og

AMESTO FORTYTWO AS
Org. nr. 991 450 068
Solheimsgaten 7A
5058 BERGEN
NORGE
(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 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 tjenester i henhold til tjenesteavtale 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.

2 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 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.

3 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 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.

4 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.

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

5 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 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, den behandlingsansvarlige skal spesifisere disse ytterligere tiltak som skal implementeres i Vedlegg C.

6 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 generell skriftlig tillatelse fra den behandlingsansvarlige.
   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 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 under-databehandlere som allerede er godkjent av den behandlingsansvarlige kan inntas i Vedlegg B.

3. 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.

4. 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 underdatabehandler-avtalen, er ikke omfattet plikten til oversendelse til den behandlingsansvarlige.

5. 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.

6. 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 and databehandleren, inkludert underdatabehandleren.

7 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:
    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 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 benyttes som grunnlag som overføringsgrunnlag etter kapittel V i GDPR.

8 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. I tillegg til databehandlerens plikt til å bistå den behandlingsansvarlige i henhold til punkt 6.4., databehandleren skal videre, hensyntatt arten av behandlingen and 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.

3. 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.

9 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 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:
    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.

10 Sletting og retur av data

Ved opphør av bestemmelsene om tjenestene knyttet til behandling av personopplysninger, er databehandleren forpliktet til å tilbakelevere alle personopplysningene til den behandlingsansvarlige og sletter eksisterende kopier, med mindre unionsretten eller Medlemsstatenes nasjonale rett krever at personopplysningene lagres.

11 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.

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.

12 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.

13 Start og opphør

1. Kontraktsbestemmelsene skal gjelde fra 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 knyttet til behandling av personopplysninger fra databehandleren. 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 bestemmelser om behandling av personopplysninger sies opp, og person-opplysningene slettes eller tilbakeleveres til den behandlingsansvarlige etter punkt 11.1. og Vedlegg C.4, Kontraktsbestemmelsene kan sies opp med skriftlig varsel fra en av partene til den andre part.

Signatur

For den behandlingsansvarlige
Navn: [NAVN]
Stilling: [STILLING]
Dato: [DATO]
Signatur: [SIGNATUR]

For databehandleren
Navn: Lena Øien
Stilling: CEO, AMESTO FORTYTWO AS
Dato:
Signatur:

14 Den behandlingsansvarliges og databehandlers kontaktopplysninger

5. Partene kan kontakte hverandre ved følgende kontakter/kontaktpunkter:

6. 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: LENA ØIAN
   Stilling: CEO, AMESTO FORTYTWO AS
   Telefon: +47 924 63 298
   E-post:lena.oian@amesto.no

Vedlegg A: Informasjon om behandlingen

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

Formålet med behandlingen er å bistå med brukerstøtte, vedlikehold og drift av leverte produkter og tekniske løsninger på vegne av behandlingsansvarlig. Også der behandlingsansvarlig gir databehandler øvrige enkeltoppdrag eller prosjekt mot samme løsning(er).

Det fører til at databehandleren kommer til å behandle personopplysninger med:

- tidsbegrenset tilgang fra egen datamaskin
- tilgang fra egen datamaskin
- midlertidig og tidsbegrenset lagring/behandling av personopplysninger, for eksempel på datamaskin eller Azure.
- lagring/behandling av personopplysninger utenfor den behandlingsansvarliges miljø, i for eksempel Azure.

A.2. Databehandlerens behandling av personopplysninger på oppdrag fra behandlingsansvarlig skal i hovedsak gjelde (behandlingens art):

Behandlingen gjelder tilgang til den behandlingsansvarliges personopplysninger. Formålet med behandlingen er *ikke* å behandle, bearbeide eller samle inn personopplysninger, annet enn i unntakstilfeller, for eksempel ved vasking eller import av personopplysninger.

Ved arbeid med den behandlingsansvarliges mottatte tjenester og støtte av disse med tilhørende apper, rapporteringsløsninger, integrasjoner og lignende, vil databehandleren få tilgang til personopplysninger, tilkoblet eller i databehandlerens eget miljø.

A.3. Behandlingen inkluderer følgende typer personopplysninger om den registrerte, men de kan variere etter hvilken type personopplysninger behandlingsansvarlig har lagret i sine systemer:

Kontaktinformasjon, som: for- og etternavn, telefonnummer, adresse, e-postadresse, fødselsdato, ansettelsesforhold og så videre

Den behandlingsansvarliges kunder og øvrige interessenters ansatte: Tittel, arbeidsgiver, interesser, løpende kommunikasjon i form av hendelser og dokumenter/e-post og så videre.

I forekommende tilfeller med HRM-system: Den ansattes navn, e-postadresse, mobiltelefon, ansattnummer, rolle, tittel, leder, forretningsområde, arbeidssted, personnummer og så videre.

Dersom særlige opplysninger ut over dette angis det i tabell under:

☐	Særlige kategorier av personopplysninger i henhold til GDPR artikkel 9 (1): <Angi type, f.eks. helseopplysninger, rasemessig eller etnisk opprinnelse eller fagforeningstilhørighet>
☐	Andre opplysninger med særlig behov for beskyttelse: <Angi type, f.eks. fødselsnummer, opplysninger om økonomi, prestasjonsvurderinger i ansettelsesforhold osv.>
☐	Andre personopplysninger: <Angi type, f.eks. navn og kontaktinformasjon, utdanning, kommunikasjonspreferanser osv.>

A.4. Behandlingen inkluderer følgende kategorier av registrerte, men de kan variere etter hvilken type personopplysninger behandlingsansvarlig har lagret i sine systemer:

- Den behandlingsansvarliges sluttbrukere.
- Den behandlingsansvarliges kunder, potensielle kunder og øvrige interessenters ansatte.
- Ansatte hos kunden.

A.5. Databehandlerens behandling av personopplysninger på oppdrag fra behandlingsansvarlig kan gjennomføres når klausulene trer i kraft. Behandlingen har følgende varighet:

BEHANDLING / TILGANG	LAGRING AV PERSONOPPLYSNINGER ELLER TILGANG	JA	NEI
Fra egen datamaskin, med tidsbegrenset tilgang styrt av behandlingsansvarlig, for eksempel i forbindelse med brukerstøtte, design, teknologi eller utvikling.	Ingen personopplysninger lagres. Tilgangen avsluttes umiddelbart etter at økten er avsluttet.	X	
Fra egen datamaskin, via databehandlers egen pålogging, for eksempel i forbindelse med brukerstøtte, design, teknologi eller utvikling.	Ingen personopplysninger lagres. Påloggingsinformasjonen slettes når avtalen utløper, når ansatte slutter eller når behandlingsansvarlig ber om det.	X	

Midlertidig og tidsbegrenset lagring/behandling av personopplysninger utenfor den behandlingsansvarliges miljø, for eksempel på datamaskin, e-post eller server hos Amesto.	Slettes 30 dager etter at oppdraget / tjenesteleveransen er godkjent eller når behandlingsansvarlig ber om det.	X	
Ikke-tidsbegrenset lagring/behandling av personopplysninger utenfor den behandlingsansvarliges miljø, i for eksempel Azure.	Slettes 30 dager etter at oppdraget / tjenesteleveransen er avsluttet eller når behandlingsansvarlig ber om det.	X	

Vedlegg B: Godkjente underleverandører

B.1. Godkjente underleverandører

Når klausulene trer i kraft, godkjenner behandlingsansvarlig at følgende underleverandører brukes:

NAVN	ORGANISASJON SNR.	LAND	BESKRIVELSE AV BEHANDLINGEN
Søsterselskap tilknyttet Amesto TechHouse		Norge, Sverige og Danmark	Amesto Fortytwo AS kan benytte konsulenter fra søsterselskap som konsulenter i prosjektet der dette løser et behov. Trust Center https://www.amesto.com/amesto-trust-center/
Microsoft		Norge, EU/EØS	Datasenter med Microsoft Cloud produkter (Azure, Microsoft 365). Datasenter region «EU West» og/eller «Norway East» benyttes med mindre annet avtalt. Trust Center https://www.microsoft.com/nb-no/trust-center
First IT		Norge	Lokalt datasenter tilbyder på Vestlandet. Tilgangskontroll for Amesto Fortytwo benyttede lokaler. Personvernerklæring https://www.firstit.no/Personvernerkl%C3%A6ring%20for%20First%20IT.pdf
Atlassian Pty Ltd		Globalt	Confluence av Atlassian benyttes for dokumentasjon. Trust Center https://www.atlassian.com/trust
TeamViewer GmbH		Globalt	TeamViewer benyttes ved behov for fjernstyring av pc klient. Må aksepteres av mottaker. Ingen varig tilknytning eller

			datafangst utover den enkelte fjernstyringssesjon for supportoppdrag. Trust Center https://www.teamviewer.com/en/trust-center/
Rubrik		Norge	Kun etter avtale. Sikkerhetskopi / backuptjeneste levert med kjøpt, dedikert utstyr plassert i lokalt datasenter med tilknytted drift og support. Kun telemetri data og teknisk lisensvalidering deles med Rubrik som innebygget del av tjenesten. Trust Center https://www.rubrik.com/trust
FortiNet		Norge, Global	Kun etter avtale. Nettverksutstyr. Leveres til kundes eie og oppsett eller som løpende driftstjeneste med sentral Cloud Management. Enkelte tjenester som DNS filter levers som tjeneste fra FortiNet direkte. GDPR Compliance https://www.fortinet.com/corporate/about-us/gdpr
Tech Data		Norge, Global	Tech Data er vår Software-distributør for Microsoft produkter.

Når klausulene trer i kraft, skal den behandlingsansvarlige godkjenne bruken av disse underleverandørene i forbindelse med den behandlingen som beskrives for parten. Med mindre det foreligger skriftlig tillatelse fra den behandlingsansvarlige, har ikke databehandleren rett til å engasjere en underleverandør i forbindelse med annen behandling enn den som er godkjent, eller la en annen underleverandør utføre den oppgitte behandlingen.

B.2. Forhåndsinformasjon om godkjenning av underleverandører

Underleverandører må godkjennes skriftlig før de kan brukes til oppgitt behandling.

Vedlegg C: Instruksjoner for behandling av personopplysninger

C.1. Omfanget av/instrukser for behandlingen

Forpliktelser som databehandler

Databehandler skal kun behandle personopplysninger i den utstrekning det er nødvendig for å oppfylle sine oppgaver og forpliktelser etter Hovedavtale eller beskrevet oppdrag.

Konfidensialitet og Taushetsplikt

Databehandleren skal sikre at autoriserte personer er forpliktet til å behandle personopplysningene fortrolig, eller er underlagt lovfestet taushetsplikt. Dette er gjort gjennom signert taushetserklæring som inngås ved ansettelse i Amesto.

Plikten til konfidensialitet gjelder også etter at databehandleroppdraget er fullført.

Databehandleren skal kun autorisere personer som av nødvendige grunner må ha tilgang til personopplysningene.

Dersom Instruks er i strid med gjeldende regler, og Behandlingsansvarlig er informert om dette, men Behandlingsansvarlig anser dette som nødvendig håndtering, for å fullføre oppdrag, vil ansvar for behandling ligge hos Behandlingsansvarlig.

Behandlingsansvarlig har ansvaret for tilgangskontroll og oppsett av tilganger i løsningen.

C.2. Sikkerhet ved behandlingen

Databehandleren treffer alle tiltak som er nødvendige etter personopplysningsloven artikkel 32. *Sikkerhet ved behandling*.

Godkjent Amesto-datamaskin i henhold til Amesto Sikkerhets Policy betyr blant annet at arbeidsstasjon låser ute andre, kun gyldig konto får logget på enheten. Benytter Remote Wipe ved tapt datamaskin for å sikre innhold.

Henviser til Amesto Personvernerklæring punkt 3. https://www.amestosolutions.no/om-oss/personvernerklaring/

Overføring av data som inneholder personopplysninger fra Behandlingsansvarlig til databehandler skal skje ved bruk av sikre overføringssystemer, etter avtale med Behandlingsansvarlig.

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:

Fysisk beskyttelse

For skyløsninger bruker Amesto Fortytwo leverandørens datasentre til lagring av informasjon. De kjører døgnet rundt og sikrer operasjoner ved å beskytte mot strømbrudd, fysisk inntrenging og

nettverksbrudd. For mer detaljer rundt underleverandørens tiltak, se «Vedlegg B: Godkjente underleverandører».

Overvåking og beskyttelse

Amesto Fortytwo leverte tjenester inkluderer avtalte driftsrutiner rundt monitorering og oppfølging. Nivået for overvåking og beskyttelse er angitt i gjeldende kontrakt.

C.4. Fremgangsmåte for lagringstid/sletting

BEHANDLING / TILGANG	LAGRING AV PERSONOPPLYSNINGER ELLER TILGANG
Fra egen datamaskin tidsbegrenset tilgang, gitt av behandlingssansvarlig, for bistand knyttet til f.eks. support, design, teknisk- eller utvikling	Ingen personopplysninger lagres. Tilgang avsluttes umiddelbart etter fullført oppdrag
Fra egen datamaskin for tilgang, gitt av behandlingssansvarlig, for bistand knyttet til f.eks support, design, teknisk- eller utvikling	Ingen personopplysninger lagres. Tilgangsinformasjon slettes i sammenheng med oppsigelse av avtale, når ansatt i Amesto Fortytwo slutter i sin stilling eller ved krav fra Behandlingsansvarlig
Midlertidig og tidsbegrenset lagring/behandling av personopplysninger utenfor behandlingsansvarlig sitt eget miljø, på f.eks datamaskin, mail, server hos Amesto	Slettes 30 dager etter oppdraget er godkjent eller etter krav fra behandlingsansvarlig
Ikke tidsbegrenset lagring/behandling av personopplysninger utenfor behandlingsansvarlig sitt eget miljø. I f.eks Azure, Amesto Flow - Saas	Slettes 30 dager etter oppdraget er godkjent eller etter krav fra behandlingsansvarlig

C.5. Behandlingssted

Behandling skjer i kundes driftsmiljø innen EU/EØS. Amesto Fortytwo har egne kontorer og arbeidssted lokalisert i Norge.

Dersom lokasjon er utenfor EU/EØS (Tredjeland) eller endringer av lokasjon endres fra det som er angitt her, skal det håndteres ihht. Databehandleravtalens punkt 7.

C.6 Instruksjoner for overføring av personopplysninger til tredjeland

Databehandleren skal kun behandle personopplysninger i tråd med dokumentert instruks fra den behandlingsansvarlige, inkludert instrukser for overføring av personopplysninger til tredjeland eller internasjonale organisasjoner, med mindre det kreves av EU-lovgivning eller nasjonal lovgivning i medlemslandet, databehandleren er underlagt. I slike tilfeller varsler databehandleren den behandlingsansvarlige om dette rettslige kravet før behandlingen, med mindre den aktuelle

lovgivningen forbyr slik varsling av hensyn til viktige samfunnsmessige interesser i samsvar med artikkel 28, punkt 3, bokstav a.

Hvis den behandlingsansvarlige ikke gir en dokumentert instruks for overføring av personopplysninger til tredjeland i disse bestemmelsene eller senere, er ikke databehandleren forpliktet til å gjennomføre slike overføringer innenfor rammene for disse bestemmelsene.

C.7 Prosedyrer for den behandlingsansvarliges kontroll, inkludert inspeksjoner, av behandlingen av personopplysninger som er overlatt til databehandleren

Ved skriftlig forespørsel skal databehandleren gi den behandlingsansvarlige dokumentasjon på de tekniske og organisatoriske tiltakene som er iverksatt for å sikre egnet sikkerhetsnivå samt annen informasjon som er nødvendig for å dokumentere at databehandleren overholder personvernforordningen, personvernbestemmelser i annen EU-lovgivning eller nasjonal lovgivning i medlemslandet, og disse bestemmelsene.

Den behandlingsansvarlige har rett til å, for egen regning, innhente en revisjonserklæring fra uavhengig tredjepart en gang i året. Behandlingsansvarlig skal dekke alle utgifter i forbindelse med kontrollen, og databehandleren har rett til kompensasjon for alle omkostninger som oppstår som følge av kontrollen, inkludert kompensasjon for rimelig medgått tid for databehandleren og dennes medarbeidere i forbindelse med bistand under kontrollen. Men databehandleren skal dekke omkostningene hvis kontrollen avdekker vesentlige mangler ved utførelsen av de forpliktelsene som kommer frem av disse bestemmelsene eller personopplysningslovgivningen.

Med utgangspunkt i resultatene fra erklæringen har den behandlingsansvarlige rett til å be om at det iverksettes ytterligere tiltak for å sikre overholdelse av personvernforordningen, personvernbestemmelser i annen EU-lovgivning eller nasjonal lovgivning i medlemslandet og i disse bestemmelsene.

Vedlegg D: Partenes regulering av andre forhold

D.1. Melding om brudd på personopplysningssikkerheten

Databehandler skal yte rimelig bistand slik at Behandlingsansvarlig kan oppfylle sine forpliktelser til å gi utfyllende informasjon til relevant tilsynsmyndighet og de registrerte.

D.2. Melding om brudd på personopplysningssikkerheten

Databehandler skal iverksette nødvendige og tilrådelige korrigerende tiltak. Databehandler skal også samarbeide med Behandlingsansvarlig for å forebygge, minimere konsekvensene av eller korrigere Sikkerhetsbrudd**.**

D.3. Ansvar

Ingen part skal overfor den annen part være ansvarlig for indirekte tap eller følgeskader av noen art (inkludert, men ikke begrenset til tap som følge av driftsavbrudd, tap av data, tapt fortjeneste eller lignende) uavhengig av ansvarsgrunnlag, hva enten i kontrakt, culpaansvar, produktansvar eller annet, selv om parten er underrettet om muligheten for slike skader (i fellesskap omtalt som "Indirekte Tap").

Ingen part skal være ansvarlig overfor den annen part for;

a) feil eller forsinkelser som ligger utenfor partens rimelige kontroll, herunder generelle internett eller linjeforsinkelser, strømbrudd eller feil på maskiner; eller

b) feil forårsaket av den annen parts systemer eller handlinger, uaktsomhet eller unnlatelser, som alene skal være den partens ansvar.

Det totale og maksimale ansvaret for hver tolv (12) måneders periode, for en part overfor den annen part under eller i medhold av denne Databehandleravtalen, skal under ingen omstendighet overstige et beløp tilsvarende det totalbeløp betalt for Tjenesten under Avtalen i løpet av de tolv (12) siste månedene forut for den skadevoldende handlingen.

Ovennevnte begrensninger skal ikke gjelde for skader som skyldes svindel, grov uaktsomhet eller forsett.

Simplifying business.

amesto
Fortytwo

Amesto Fortytwo
Solheimsgaten 7A
5058 Bergen