Databehandleravtale

Sikri AS («**Databehandler**» eller «**Sikri**»)

Org.nr. 922 308 055

og

Modalen kommune

Org.nr 964 969 302.

(«**Behandlingsansvarlig**» eller «**Kunde**»)

Datert 31 oktober 2023

Sikri AS

Hege Moe Tveit

Modalen kommune

Jo Bjarte Tømmerbakke
Rådmann

Avtalen signeres i to eksemplarer, ett til hver av partene.

1. Omfanget av avtalen

Kunden og Sikri har inngått en avtale angående vedlikehold av programvare for Sak- og arkivsystemer.

I forbindelse med levering av tjenester i henhold til gjeldende avtale må Sikri behandle personopplysninger på vegne av kunden eller kundens kunder. For å sikre at alle personlige data til enhver tid behandles i samsvar med gjeldende lov, er partene enige om å inngå denne Databehandleravtalen **(DBA)**.

I tilfelle konflikt mellom DBA og Hovedavtale, skal DBA gjelde.

Når det henvises til Sikri i denne DBA, skal dette også gjelde for Sikris samarbeidspartnere samt enhver annen underbehandler som er tillatt i denne DBA. Når det henvises til kunden i denne DBA, skal dette også gjelde for kundens kunder.

2. Definisjoner

«Datterselskap» til en part: alle juridiske personer som (i) direkte eller indirekte eier eller kontrollerer parten, (ii) har samme direkte eller indirekte eierforhold eller kontroll som parten, eller (iii) direkte eller indirekte styres av parten så lenge som slike eierforhold eller kontrollforhold varer. Eierskap eller kontroll skal foreligge gjennom direkte eller indirekte eierskap på femti prosent (50 %) eller mer av den nominelle verdien av den utstedte eierandelskapitalen eller på femti prosent (50 %) eller mer av aksjene som gir innehaveren rett til å stemme ved valg av styremedlemmer eller personer som utfører lignende funksjoner.

«**Gjeldende lov**»: lovverk som er i kraft (for eksempel gjeldende personopplysningslov (Lov 2018-06-15-38), personopplysningsforskriften, generell personvernforordning / GDPR - (EU) 2016/679).

«**Behandlingsansvarlig**»: en fysisk eller juridisk person, en offentlig myndighet, en institusjon eller ethvert annet organ som alene eller sammen med andre bestemmer formålet med behandlingen av personopplysninger og hvilke midler som skal benyttes; når formålet med og midlene for behandlingen er fastsatt i unionsretten eller i medlemsstatenes nasjonale rett, kan den behandlingsansvarlige, eller de særlige kriteriene for utpeking av vedkommende, fastsettes i unionsretten eller i medlemsstatenes nasjonale rett.

«**Personopplysninger**»: enhver opplysning om en identifisert eller identifiserbar fysisk person; en identifiserbar fysisk person er en person som direkte eller indirekte kan identifiseres, særlig ved hjelp av en identifikator, f.eks. et navn, et identifikasjonsnummer, lokaliseringsopplysninger, en nettidentifikator eller ett eller flere elementer som er spesifikke for nevnte fysiske persons fysiske, fysiologiske, genetiske, psykiske, økonomiske, kulturelle eller sosiale identitet.

«Særlige kategorier personopplysninger»: personopplysninger om rasemessig eller etnisk opprinnelse, politisk oppfatning, religion, overbevisning eller fagforeningsmedlemskap, samt behandling av genetiske opplysninger og biometriske opplysninger med det formål å entydig identifisere en fysisk person, helseopplysninger eller opplysninger om en fysisk persons seksuelle forhold eller seksuelle orientering.

«**Brudd på personopplysningssikkerheten**»: et brudd på sikkerheten som fører til utilsiktet eller ulovlig tilintetgjøring, tap, endring, ulovlig spredning av eller tilgang til personopplysninger som er overført, lagret eller på annen måte behandlet.

«**Databehandler**»: en fysisk eller juridisk person, offentlig myndighet, institusjon eller ethvert annet organ som behandler personopplysninger på vegne av den behandlingsansvarlige.

«**Behandling**» **eller «(å) behandle**»: enhver operasjon eller rekke av operasjoner som gjøres med personopplysninger, enten automatisert eller ikke, f.eks. innsamling, registrering, organisering, strukturering, lagring, tilpasning eller endring, gjenfinning, konsultering, bruk, utlevering ved overføring, spredning eller alle andre former for tilgjengeliggjøring, sammenstilling eller samkjøring, begrensning, sletting eller tilintetgjøring.

«**Underleverandør**»: en hvilken som helst underleverandør som behandler personopplysninger på vegne av Sikri eller en hvilken som helst annen underleverandør.

3. Sikri sine forpliktelser

3.1 Generelt

Sikri forplikter seg til å behandle personopplysninger kun i samsvar med gjeldende lov, denne DBA og kundens dokumenterte instruksjoner.

Sikri kan ikke:

a) samle inn eller offentliggjøre personopplysninger fra eller til en tredjepart (unntatt i henhold til det som beskrives i denne DBA)
b) endre behandlingsmåten
c) kopiere eller reprodusere personopplysninger
d) kompilere eller sortere personopplysninger
e) på annen måte behandle personopplysninger for andre formål enn de som er angitt i vedlegg 1, Hovedavtalen og denne DBA

Sikri har utpekt en personvernansvarlig for å overholde rutiner for å ivareta at personopplysninger behandles i samsvar med Sikris interne rutiner og kundens instruksjoner.

Sikri skal utføre kontroll av alle kategorier av behandlingsaktiviteter utført på vegne av kunden, som inneholder: a) navn og kontaktinformasjon til Sikri og personvernansvarlig; b) kategorier av behandling utført på vegne av kunden; c) eventuell overføring av personopplysninger til et tredje land, inkludert identifikasjon av det tredje land, og eventuelt registrering av egnede beskyttelsestiltak; og d) der det er mulig; en generell beskrivelse av de tekniske og organisasjonsmessige sikkerhetstiltak.

Sikri skal etter nærmere avtale bistå kunden med å utføre en personvernkonsekvensvurdering (også kjent som Data Protection Impact Assessment) om ønskelig. Sikri skal på samme måte etter anmodning bistå med å sikre at krav til innebygd personvern i Sikris løsninger innfris. Dette inkluderer å bygge inn funksjonalitet for å oppfylle personvernprinsipper samt funksjonalitet for å sikre den registrertes rettigheter (så langt det med rimelighet kan forventes med hensyn til formålet med løsningen).

3.2 Tekniske, organisatoriske og sikkerhetsmessige tiltak

Idet det tas hensyn til tilgjengelig teknologi, kostnader for gjennomføring samt art, omfang, kontekst og formålet med behandlingen så vel som risikoen for varierende sannsynlighet og alvorlighetsgrad for rettigheter og friheter hos fysiske personer, skal Sikri iverksette hensiktsmessige tekniske og organisatoriske tiltak for å sikre et sikkerhetsnivå som passer til risikofaktoren i henhold til Hovedavtalen. Slike tiltak kan blant annet omfatte: a) pseudonymisering og kryptering av personopplysninger; b) muligheten til å sikre løpende konfidensialitet, integritet, tilgjengelighet og robusthet i behandlingssystemer og -tjenester; c) evne til å gjenopprette tilgjengelighet og tilgang til personopplysninger så raskt som mulig i tilfelle fysiske eller tekniske hendelser; og d) en fremgangsmåte for regelmessig testing, vurdering og evaluering av effektiviteten til tekniske og organisasjonsmessige tiltak for å sikre at sikkerheten ivaretas under behandlingen.

Ved vurderingen av riktig nivå av sikkerhet skal det tas spesielt hensyn til risikoen knyttet til avtalte tjenester om behandling, spesielt i forbindelse med utilsiktet eller ulovlig tilintetgjøring, tap, endring, ulovlig spredning av eller tilgang til personopplysninger som er overført, lagret eller på annen måte behandlet.

Ved behandling ved hjelp av ny teknologi skal det tas spesielt hensyn til art, omfang, kontekst og formål da det trolig vil resultere i en høy risiko for de rettigheter og friheter som fysiske personer har. I slike tilfeller skal Sikri, hvis instruert av kunden, bistå med sin vurdering av virkningen av den planlagte behandlingen på beskyttelse av personopplysninger.

Sikri forplikter seg til å sikre at involvert personell hos Sikri blir gjort oppmerksom på og følger Sikris forpliktelser i henhold til denne DBA.

3.3 Kontroll og gjennomgang

Kunden kan kreve en årlig kontroll og gjennomgang. Kontroll og gjennomgang kan også kreves og gjennomføres av en relevant myndighet på grunn av juridiske krav eller på annen måte som en del av Sikris interne forretningsrutiner. Kunden kan når som helst, etter varsel gitt i rimelig tid, selv granske Sikris samsvar med vilkårene i denne DBA. I forbindelse med en slik revisjon skal kunden gis tilgang til Sikris lokaler, datautstyr, sikkerhetspolicyer og lignende i den grad det er nødvendig for å utføre kontroll og gjennomgang (men det skal ikke gis tilgang til informasjon om Sikris øvrige kunder og annen informasjon underlagt taushetsplikt). En kundeinitiert kontroll og gjennomgang, skal faktureres basert på tid og materiell. Ved anmodning fra en av partene skal personer/parter som får tilgang til informasjon av Sikri, undertegne en taushetserklæring som omfatter kontrollen og gjennomgangen.

3.4 Hendelseshåndtering og varsling ved brudd på personopplysningssikkerhet

Sikri skal, idet det tas hensyn til behandlingsarten og tilgjengelig informasjon, bistå kunden i å sikre etterlevelse av forpliktelsene vedrørende sikkerheten ved behandling av personopplysninger.

I tilfelle brudd på personopplysningssikkerheten skal Sikri straks, uten ugrunnet opphold, varsle kunden om bruddet på personopplysningssikkerheten. Varsel om brudd på personopplysningssikkerheten skal som minimum: a) beskrive omfanget av bruddet på

personopplysningssikkerheten inkludert, der hvor det er mulig, kategorier og omtrentlig antall registrerte som er berørt, samt kategorier og omtrentlig antall berørte personlige dataposter; b) kommunisere navnet og kontaktinformasjon til personvernansvarlig eller annet kontaktpunkt hvor mer informasjon kan hentes; c) beskrive de sannsynlige konsekvensene av bruddet på personopplysningssikkerheten; d) beskrive de tiltakene som iverksettes eller foreslås iverksatt for å håndtere bruddet på personopplysningssikkerheten, blant annet, når det er hensiktsmessig, tiltak for å redusere mulige uønskede bivirkninger; og e) enhver annen nødvendig og rimelig tilgjengelig informasjon som kunden trenger for å være i stand til å treffe hensiktsmessige tiltak og oppfylle sine forpliktelser for varsling om bruddet på personopplysningssikkerheten til relevante tilsynsmyndigheter.

Sikri skal dokumentere bruddet på personopplysningssikkerheten, inkludert en redegjørelse for de faktiske forhold knyttet til bruddet, dets virkninger og eventuelle iverksatte utbedringstiltak.

3.5 Støtte og informasjon til registrerte enkeltpersoner og tilsynsmyndigheter

I tilfeller der en registrert person, en tilsynsmyndighet eller tredjepart ber om informasjon relatert til personopplysninger fra Sikri, skal Sikri uten ugrunnet opphold henvise til kunden. Sikri forplikter seg til å hjelpe kunden, med det som er nødvendig for å møte forespørsler fra tilsynsmyndigheter og for å oppfylle kundens forpliktelser vedrørende individets rettigheter, inkludert, men ikke begrenset til, rett til korrigering og sletting, rett til dataportabilitet, innsigelsesrett og rett til begrensning av behandling. Databehandler vil fakturere basert på tid og materiell, dersom Behandlingsansvarlig ber om tjenester utover det å svare på enkle spørsmål eller oversendelse av dokumentasjon.

3.6 Underleverandører

Sikri kan ikke legge deler av behandlingen til en underleverandør uten skriftlig forhåndssamtykke fra kunden. Slikt samtykke kan ikke holdes tilbake uten saklig grunn. Sikri skal holde en oppdatert liste over identiteten og plasseringen av underleverandører, og den skal være tilgjengelig for kunden og relevante tilsynsmyndigheter. Endringer skal gjøres tilgjengelig for kunden i henhold til avtalte prosedyrer. Sikri vil til enhver tid være fullt ut ansvarlig for underleverandørenes etterlevelse av bestemmelsene i denne DBA.

3.7 Overføring av personopplysninger

Sikri kan overføre kundens personopplysninger til Sikris samarbeidspartnere og underleverandører i utlandet i henhold til følgende prosess:

3.7.1 Norden (Norge, Sverige, Finland og Danmark)

Overføring av personopplysninger til samarbeidspartnere og underleverandører kan skje uten ytterligere bekreftelse fra kunden når formålet er å oppfylle forpliktelser, samarbeide eller ivareta rettigheter spesifisert i avtalen, eller når kunden spesifikt har godkjent underleverandøren.

3.7.2 Innenfor EU/EØS

For overføring av personopplysninger til samarbeidspartnere og underleverandører hvor behandlingen utføres utenfor Norden, men innenfor EU/EØS, er Sikri pålagt å gi nødvendig

dokumentasjon om sikkerhet, samsvar og risiko knyttet til aktuelt selskap og plassering. Basert på slik dokumentasjon og slike beskrivelser skal kunden utarbeide en særskilt risikovurdering som skal brukes som beslutningsgrunnlag. Kunden kan ikke nekte samtykke til den aktuelle overføringen uten gyldig grunnlag basert på spesifikke risikoer som følger av kundens risikovurdering.

3.7.3 Utenfor EU/EØS

For å overholde kravene i relevant personopplysningslov for overføring av personopplysninger til samarbeidspartnere og underleverandører hvor behandlingen utføres utenfor EU/EØS, skal EUs standardkontrakter eller annet gyldig rettsgrunnlag som beskriver omfanget av engasjementet, være inngått mellom kunden og det aktuelle selskapet på stedet.

Sikri skal gi nødvendig dokumentasjon om sikkerhet, samsvar og risiko knyttet til aktuelt selskap og plassering. Basert på tilgjengelig dokumentasjon og beskrivelser skal kunden utarbeide en særskilt risikovurdering som skal brukes som beslutningsgrunnlag. Samtykke til og/eller inngåelse av dataoverføringsavtale skal ikke tilbakeholdes uten gyldig grunnlag basert på spesifikke risikoer som følger av kundens risikovurdering.

3.8 Ansvar

Ansvar i forbindelse med manglende overholdelse av Sikris forpliktelser ifølge Gjeldende lov som er spesifikt rettet mot databehandlere, eller hvor databehandleren har handlet utenfor eller i strid med lovlige instrukser fra behandlingsansvarlig, styres av Hovedavtalen, og hvis ikke, av Sikris endringsbilag til hovedavtalen. Sikri skal være fritatt for ansvar i den grad Sikri ikke er ansvarlig for, eller årsaken til, hendelsen eller omstendigheten som gir opphav til skaden.

3.9 Taushetsplikt

Sikri skal behandle og lagre personopplysninger konfidensielt. Personopplysninger kan bare nås og administreres av personell hos Sikri som trenger tilgang til opplysningene for å oppfylle Sikris forpliktelser i henhold til avtalen og denne DBA, og som har bekreftet å bevare taushet gjennom en skriftlig avtale, og bare i den grad det er nødvendig for å oppfylle Sikris forpliktelser i henhold til avtalen og denne DBA. I tillegg skal bestemmelsene om taushetsplikt fastsatt i avtalen også gjelde for denne DBA og enhver behandling.

3.10 Returnering og sletting av personopplysninger

Etter avsluttet behandling skal Sikri returnere eller, etter Kundens instruks, slette og ødelegge alle personopplysninger med opphav i Hovedavtale og DBA. Personopplysninger som kreves lagret etter forpliktelse i lov eller lovpålagt dokumenteringsformål, vil bli slettet når slikt formål er oppfylt.

4. Betingelser og endringer i DBA

Denne DBA gjelder fra signering og så lenge Sikri behandler personopplysninger som kunden har ansvar for. I tilfelle endringer i Gjeldende lov, endelig dom gir en annen tolkning av Gjeldende lov,

eller tjenestene i avtalen krever endringer av denne DBA, skal partene samarbeide i god tro for å oppdatere DBA tilsvarende.

5. Tvister og gjeldende lovverk

Partenes rettigheter og plikter reguleres av norsk rett. Alle tvister, konflikter eller krav som oppstår på grunn av eller i forbindelse med denne DBA, eller ved brudd, oppsigelse eller ugyldighet av nevnte regler og vilkår, skal avgjøres ved voldgift i samsvar med reglene i norsk voldgiftslov av 2004. Alle deler av saksbehandlingen i slike voldgiftssaker skal være konfidensielle, inkludert dommen. Oslo avtales som verneting.

Vedlegg 1: Personopplysninger

Hensikten er at dataene nedenfor danner grunnlaget for de protokoller over behandling som både behandler og behandlingsansvarlig er bundet til å opprette og holde oversikt over.

Behandlingsansvarlig	**Databehandler**
Navn Modalen kommune	Navn Sikri AS
Kontaktopplysninger melding av GDPR saker Namn: Tonje Husum Aarland Stilling: Ass. Rådmann Epost: tonje.husum.aarland@modalen.kommune.no Tlf: 92858413	Kontaktopplysninger melding av GDPR saker Epost: gdprecm@sikri.no Telefon: +47 90530049
Navn på personvernansvarlig Namn: Lars Erling Aarland – Stilling: Personvernombod Epost: lars.erling.aarland@iktnh.no Tlf: 41450043	Navn på kontaktperson Navn: Helen Indrekvam Stilling: Compliance Officer Epost: helen.indrekvam@sikri.no Telefon: +47 959 24 220
Andre kontaktopplysninger Navn: Lin Tove Thomassen Stilling: leiar kundetorget Epost: lin.tove.thomassen@modalen.kommunee.no Telefon: 98667846	Andre kontaktopplysninger Navn: Hege Moe Tveit Stilling: General director Epost: hege.tveit@sikri.no Telefon: +47 918 45 396

1. Innledende beskrivelse

Følgende er de mest relevante kontraktsfestede tjenestene og de ulike behandlingsaktivitetene der Databehandleren vil kunne behandle personopplysninger på vegne av Behandlingsansvarlig:

1.1. Leveransen og innføringsprosjektet, med installering, opplæring/kurs og testaktiviteter

1.2. Installering og/eller oppgradering over linje eller fysisk tilstedeværelse på Kundens lokasjon

1.3. Drift av løsningen med aktiviteter som backup, restore og applikasjonsrelatert vedlikehold

1.4. Registrering av arbeidsrelatert informasjon om rolle og brukeridentitet for brukere i løsningen. Utføres som en maskinell spørring for å beregne riktig pris basert på kundens forbruk

1.5. Support der Kunden oversender dokumentasjon som er relevant for feilsøking og saksbehandling

1.6. Feilsøking på kundens installasjon der databehandler aksesserer data ved autoriserte tilganger.

2. Presisering av behandlingsaktiviteter og område for behandlingen

2.1. All lagring av data gjøres innenfor EU.

3. Risikoreduserende tiltak som er satt i verk (ikke uttømmende)

3.1. Databehandler har relevante sertifiseringer relatert til miljø (ISO 14001), kvalitet (ISO 9001) og informasjonssikkerhet (ISO 27001)

3.2. Alle databehandlers ansatte har gjennomgått, repeterer jevnlig og undertegner code of conduct

3.3. Alle Databehandlers ressurser som leverer de kontraktsfestede tjenestene har fått spesialopplæring i relevante rutiner

3.4. Databehandlers ressurser som utfører de kontraktsfestede tjenestene, har signert taushetserklæringer

3.5. Databehandler vil ikke lagre data med mindre dette er som en del av de kontraktsfestede tjenestene med kunden

3.6. Det er implementert rutiner for overføring, lagring og sletting av informasjon i support og vedlikehold

3.7. Det er implementert rutiner for Databehandlers tilganger til Behandlingsansvarliges miljøer

3.8. Tilbakelevering eller sletting av data er regulert i Databehandleravtalen

3.9. Behandlingsansvarlig regulerer hvor, hvem og hvor mange som skal få tilgang til deres applikasjon.

3.10 Ved Databehandlers bruk av underleverandører skal Databehandler ta ansvar for å sikre at både kompetanse, rutiner, sertifiseringer og relevante avtaler er på plass når disse behandler personopplysninger på vegne av Behandlingsansvarlig.

4. Avstemmes av behandlingsansvarlig og databehandler

Vær vennlig å avstemme at databehandlers informasjon besvart i avkryssingsbokser og tekst i blå font som følger er korrekt.

Personopplysningene som behandles gjelder følgende kategorier av registrerte tilknyttet kunden (vennligst angi):

☒Ansatte og kontraktører
☒Sluttkunder
☐Leverandører
☐Nettstedsbesøkende
☐Fysiske besøkere
☐Andre tredjeparter (vennligst spesifiser):
.....
.....
.....
.....

Kategorier av Personopplysninger: Personopplysninger som behandles, omfatter følgende kategorier (spesifiser):

☒Personlig kontaktinformasjon – navn, telefonnummer, e-postadresse, fysisk adresse osv.
☒Begrenset kontaktinformasjon – personnummer/fødselsnummer, hemmelig adresse osv.
☒Arbeidsrelatert informasjon – stilling/rolle, organisasjon, bedrift, telefonnummer / e-post / fysisk adresse for arbeid, arbeidshistorikk (tidligere stillinger) osv.
☒ Enhetsinformasjon – merke og modell, IP-adresse, MAC-adresse, serienummer, posisjonsdata osv.
☐Kommunikasjon av data – start-/slutt-tid for kommunikasjon (økt), størrelsen på meldingen, kontekst osv.
☐Overvåking/overvåkningsdata – adgangskontroll-logger (fysiske/logiske), CCTV-opptak, kjøreovervåkningsdata osv.
☒Transkripsjoner/ kundeinteraksjoner – kundesamtaler (tale eller transkribert), supportsaker, e-postmarkedsføring, annen kundekorrespondanse osv.
☐Profileringsdata – analyser og rapporter om registrerte personer, for eksempel i markedsføringsøyemed
☐Betalingsinformasjon – finansielle transaksjoner, mottaker, kontonummer, beløp, dato / tid / sted for kjøp osv.
☐Betalingskortinformasjon– kredittkortnummer, utløpsdato, CVV-nummer, annen kortholderinformasjon osv.
☒ Annet (vennligst spesifiser):

Databehandler vil kunne, i de beskrevne behandlingsaktivitetene i innledningen til dette vedlegget, behandle personopplysninger om kunden og kunden sine kunder.

Særskilte kategorier personopplysninger som behandles, omfatter følgende spesialkategorier (spesifiser):

Personopplysninger som avslører noe av det følgende (særskilt risiko):

☐Rasemessig eller etnisk opprinnelse
☐Politiske meninger
☐Religiøs eller filosofisk overbevisning
☐Fagforeningsmedlemskap
☐Genetiske data med det formål entydig å identifisere en fysisk person
☐Biometriske data med det formål entydig å identifisere en fysisk person
☐Helseopplysninger
☐Opplysninger om en fysisk persons seksuelle forhold eller legning

Et sak- og arkivsystem vil kunne inneholde særskilte kategorier personopplysninger og legges inn i systemet av den Behandlingsansvarlige. Databehandler vil kunne, i de beskrevne behandlingsaktivitetene i innledningen til dette vedlegget, behandle særskilte kategorier personopplysninger i tjenestene dersom de ser og/eller aksesserer dette. Se innledende beskrivelse til Vedlegg 1/dette vedlegget.

Spesielle sikkerhetsbehov: Avkryssing på noen av de følgende spørsmålene, vil innebære at det må inngås en avtale om økt sikkerhet mot særskilt vederlag.

Merk: Dersom det identifiseres spesielle sikkerhetsbehov, utover det som er definert i hovedavtalen og/eller tiltak utover de som allerede er iverksatt, vil dette innebære at det må inngås avtale om økt sikkerhet der kostnader kan påløpe Kunden.

☐Særlige behov for konfidensialitet
☐Særlige behov for integritet
☐Særlige behov for tilgjengelighet
☐Særlige behov for personvernfremmende teknologier (f.eks. Innebygd personvern)

Beskriv eventuelle spesialbehov utover det som er definert i Hovedavtalen og iverksatt. Det vil kunne påløpe tilleggskostnader for Kunden relatert til dette:

.....
.....
.....
.....

Formål med behandlingen: Personopplysningene behandles for følgende formål (vennligst spesifiser):

☐Personaladministrasjon
☒ Kundebehandling
☐Leverandørhåndtering
☐Intern prosesstøtte
☒Annet (vennligst spesifiser):

Databehandlers hovedformål med behandlingen er å oppfylle kontraktsfestede tjenester i Hovedavtalen om brukerstøtte/support, feilretting og eventuelt drift.

Kategorier behandlingsaktiviteter: Personopplysningene vil være underlagt følgende behandlingsaktiviteter (vennligst spesifiser relevante tjenester; skriv inn avtale- og tjenestespesifikasjon):

Se innledende beskrivelse til Vedlegg 1/dette vedlegget om behandlingsaktivitetene knyttet til de kontraktsfestede tjenestene knyttet til brukerstøtte, feilretting og eventuelt drift av systemet.

Underleverandører som behandler personopplysninger (alle juridiske enheter, inkludert de i tredjeland eller internasjonale organisasjoner, som kan ha tilgang til og/eller på annen måte behandler personopplysninger):

Kunden samtykker i at Sikri kan bruke programvareleverandører, infrastrukturleverandører, driftsleverandører og konsulenter som er nødvendig for å gjennomføre de avtalte tjenester på like strenge vilkår og krav til sikkerhet som Sikri.

Detaljer vil være tilgjengelig for kunden og relevante tilsynsmyndigheter i tabellene nedenfor i vedlegg 1 til denne DBA.

I tillegg gis det samtykke til følgende underleverandører av Sikri vil levere en del av tjenestene ved support og vedlikehold:

Navn og org.nr	Adresse	Beskrivelse av behandling	Behand-lingsted	Kontakt informasjon	Særlige kategori er persono pplysnin ger
Visma First Agenda *Company number 3709 8922*	*Søren Frichs Vej 44D 8230 Aarhus, Danmark*	***Gjelder dersom kunde har møtemodul*** *Underleverandør på basis drift for tilgjengeliggjøring av møtedokumenter for møtedeltagere.* *Tilgang til data:* *Har tilgang til kontaktopplysninger (navn og epost) på ansatte og folkevalgte.* *I tillegg har First Agenda tilgang til alle dokumenter/informasjon som Behandlingsansvarlig selv velger å legge inn i First Agenda.*	*Danmark*	Director development Sikri E: ida.johansen@sikri.no T: +47 94287843	*Nei*
Sem & Stenersen Prokom Norge *Organisasjons nr 953 675 358*	*Karl Johans gate 37B 0162 Oslo*	***Gjelder dersom kunde har skjemaløsning*** *Behandler:* *Kontaktopplysninger* *Mellomlagrer data – det betyr data som sluttbruker lagrer ved utfylling av skjema. Mellomlagring slettes etter 30 dager.*	*Norge*	Director development Sikri E: ida.johansen@sikri.no T: +47 94287843	*Nei*

		Hovedkategorier av behandlingsaktiviteter: Driftsrelaterte oppgaver *- Yte bistand i prosjekt* *Underkategorier av behandlingsaktiviteter:* *Lagring av data, backup, loggføring, feilsøking, tilrettelegging, konsultering og vedlikehold.* *Behandling av persondata skal som hovedregel ikke være påkrevd i forbindelse med ovennevnte aktiviteter, men kan forekomme i forbindelse med håndtering av feil, testing og utvikling.*			

Følgende underleverandør av Sikri vil levere en del av tjenestene ved drift av løsningen:

Navn og org.nr	Adresse	Beskrivelse av behandling	Behandlings sted	Kontakt informasjon	Særlige kategorier personopplysninger
Microsoft Norge	*Dronning Eufemias gate 71, 0194 Oslo Norge*	*Benyttes som underleverandør av Sikri ved drift av løsningen.* *Leverandøren har tilgang til hardware. Leverandør har ikke tilgang til applikasjonslaget og kundedata. Microsoft har ikke mulighet til å gi seg selv rettigheter til pålogging/tilgang til applikasjon og kundedata.*	*Norge*	Director development Sikri E: ida.johansen@sikri.no T: +47 94287843	*Nei*

Overføring av personopplysninger til tredjeland eller til internasjonale organisasjoner:

☐Alle behandlingsaktiviteter utføres av personell i Norden.

☒Alle behandlingsaktiviteter utføres av personell i EU/EØS.

☐ Behandlingsaktiviteter kan utføres av personell utenfor EU/EØS. Kunden må inkludere slike behandlingsaktiviteter i EUs standardkontrakter, jf. SCC (Standard Contractual Clauses).

Passende sikkerhet for overføring til tredjeland eller internasjonal organisasjon:
På vegne av kunden **BEKREFTER** jeg at EUs standardkontrakter er undertegnet av kompetent person og vedlagt til denne avtalen.

Det utføres ikke behandlingsaktiviteter utenfor EU/EØS.

Oppbevaringsperioder for de forskjellige kategorier av personopplysninger (eller kriterier for å bestemme slike oppbevaringsperioder):

.....

Hvis ikke annet er avtalt, vil Sikri oppbevare kundens personopplysninger i perioden angitt i hovedavtalens varighetsperiode.