Databehandleravtale

Databehandleravtale
Inngår i samme avtaleinngåelse som salgsavtalen og brukervilkårene
Oppdatert 18. oktober 2026

Databehandleravtale etter personvernforordningen (GDPR) artikkel 28. Dette dokumentet er vedlegg 2 til salgsavtalen eller den bekreftede nettbestillingen («hovedavtalen»).
Et hus er et avgrenset område i Demokratiappen der en virksomhet inviterer deltakere til sin aktivitet. Denne avtalen regulerer Leverandørens behandling på Kundens vegne. Henvisninger til vedlegg A–D gjelder underdelene i denne databehandleravtalen. Den ordinære bestillingen og avtaleoversikten utfyller disse med Kundens avtalte bruk og instrukser. Kunden laster opp og vedlikeholder sin egen personvernerklæring for huset. Erklæringen erstatter ikke databehandleravtalen. Berørt behandling skal ikke starte før instruksen, nødvendige leverandørgodkjenninger og deltakerinformasjonen er på plass.

1. Parter og hovedavtale

Opplysning	Behandlingsansvarlig («Kunden»)	Databehandler («Leverandøren»)
Juridisk navn	Kunden identifisert i hovedavtalen.	Okasi 1 AS
Organisasjonsnummer	Som angitt i hovedavtalen.	933 731 103
Adresse	Som angitt i hovedavtalen.	Thormøhlens gate 51, 5006 Bergen
Kontakt for personvern	Personvernkontakten i hovedavtalens bestilling eller avtaleoversikt.	support@demokratiapp.no
Kontakt for sikkerhetsavvik	Avvikskontakten og eskaleringskanalen i hovedavtalens bestilling eller avtaleoversikt.	support@demokratiapp.no. Ved hastesak benyttes også avtalt telefon-/eskaleringskanal i bestillingen.
Personvernombud, hvis relevant	Ombudskontakten i hovedavtalen eller avtaleoversikten, dersom Kunden har oppnevnt ombud.	Personvernkontakt: support@demokratiapp.no.

Partene, kontaktopplysningene og datoen for avtaleinngåelsen følger hovedavtalen eller den bekreftede nettbestillingen og gjenbrukes her uten ny utfylling. Avtaleoversikten identifiserer berørte hus, juridiske enheter, avtalt bruk og de dokumentversjonene og underdatabehandlergodkjenningene som følger avtalen. Denne avtalen med vedlegg A–D inngår sammen med hovedavtalen og brukervilkårene i vedlegg 1 gjennom samme signering eller dokumenterte elektroniske avtaleinngåelse etter punkt 2. En senere nettsideendring eller opplasting av Kundens personvernerklæring endrer ikke instruksen. Dersom Kunden selv er databehandler, skal dette fremgå av hovedavtalen, og Kundens fullmakt fra den behandlingsansvarlige skal være dokumentert. Leverandøren opptrer da som underdatabehandler.

2. Formål, roller og varighet

Leverandøren behandler opplysningene for å levere funksjonene Kunden har bestilt innenfor hovedavtalen og brukervilkårene i vedlegg 1: administrere hus, medlemmer og roller, gjennomføre avstemninger og undersøkelser, håndtere ideer, problemer, kunngjøringer, arrangementer og dokumenter samt nødvendig drift, støtte, eksport og sletting. Bare konkret avtalte aktiviteter, formål, opplysningskategorier, registrerte, tilganger og frister i vedlegg A

og D omfattes. Tilgang til en funksjon er ikke instruks om all behandling funksjonen kan brukes til.

Kunden bestemmer formålet med behandlingen i sitt hus, hvilke deltakere som omfattes, hvilke spørsmål som stilles, og hvem som får se opplysninger og resultater. Leverandøren bestemmer ikke at Kundens innhold skal brukes til egne analyser, annonsering eller trening av KI-modeller. Slik bruk er ikke tillatt etter denne avtalen. Anonymisering av Kundens data krever også dokumentert instruks; et ønske om «anonym statistikk» gir ikke en generell rett til å gjenbruke data.

Leverandørens separate behandling for personlig brukerkonto, egne kjøp, kontaktpersoner, bokføring og egne dokumenterte sikkerhetsformål beskrives i personvernerklæringene. At data ligger på samme plattform, gjør ikke all behandling til Leverandørens selvstendige ansvar. Kundespesifikke logger og supportdata behandles under denne avtalen når de behandles på Kundens vegne. Rollene bestemmes av faktisk behandling, ikke av etiketten i en avtale.

Databehandleravtalen med vedlegg A–D inngås sammen med hovedavtalen, uten separat signering eller aksept. Ved signert salgsavtale trer den i kraft når begge parter har signert, med datoen for siste signatur som ikrafttredelsesdato. Ved ordinær nettbestilling som tillates etter brukervilkårene, inngås den gjennom Kundens dokumenterte elektroniske aksept og Leverandørens ordrebekreftelse. Den aktuelle dokumentversjonen med fullstendige vedlegg A–D skal være innlemmet, tilgjengelig før aksept og følge ordrebekreftelsen; avtalen trer da i kraft når ordrebekreftelsen er sendt etter Kundens aksept. Har hovedavtalen uttrykkelig krav om begge parters signatur, gjelder dette. Avtalen skal være bindende før Leverandøren behandler personopplysninger på Kundens vegne, og gjelder så lenge Leverandøren eller underdatabehandlere behandler dem, også ved avvikling og i sikkerhetskopier. Taushetsplikten gjelder også etter opphør. Ved motstrid går denne databehandleravtalen foran hovedavtalen og brukervilkårene i spørsmål om behandling av personopplysninger. Ufravikelig rett og eventuelle bindende standard personvernbestemmelser går foran.

3. Kundens plikter og instrukser

Kunden er ansvarlig for gyldig behandlingsgrunnlag, informasjon til deltakerne og nødvendig begrensning av innsamling og lagring. Kunden beskriver og bekrefter den avtalte bruken i den ordinære bestillingen og gir dokumenterte instrukser etter vedlegg A og D. Kunden laster opp og publiserer en korrekt, oppdatert personvernerklæring som faktisk dekker bruken av huset, og oppgir personvernkontakt. Kunden vurderer behovet for personvernkonsekvensvurdering (DPIA), personvernombud og eventuell forhåndsdrøfting med Datatilsynet. Kundens avtaleaksept og deltakernes bekreftelse på mottatt informasjon er ikke samtykke eller i seg selv behandlingsgrunnlag for deltakernes opplysninger.

Ved politiske oppfatninger, partimedlemskap, fagforeningsforhold, helseopplysninger eller andre særlige kategorier skal Kunden både dokumentere grunnlag etter artikkel 6 og et anvendelig unntak i artikkel 9. Artikkel 9 nr. 2 bokstav d kan være relevant for et politisk eller fagforeningsmessig organ innenfor bestemmelsens rammer; den gir ikke fri adgang til deling mellom selvstendige juridiske enheter eller til allmennheten. Samtykke må være reelt frivillig og er normalt lite egnet i avhengighetsforhold. Offentlige myndigheter kan ikke bruke berettiget interesse som grunnlag når de utfører sine offentlige oppgaver.

Hovedavtalens avtaleoversikt og vedlegg A–D utgjør Kundens dokumenterte instruks. Kunden holder fakta og instrukser oppdatert gjennom avtalte skriftlige kanaler og valg i tjenesten innenfor avtalens rammer. Bare personer med fullmakt etter vedlegg D kan gi vesentlige nye instrukser. En administratorrolle gir ikke i seg selv fullmakt til å fravike avtalen eller godkjenne nye behandlingsformål. Endret formål, nye opplysningskategorier, utvidet deling eller bruk av selvstendige juridiske enheter skal avklares og dokumenteres før den nye behandlingen starter. En ny personvernerklæring alene endrer verken instruksen eller tjenestens lagrings- og sletteinnstillinger.

Kunden kan uttrykkelig knytte samme opplastede erklæring til flere hus under samme juridiske behandlingsansvarlige når erklæringen dekker bruken i alle husene. Samme avtalte instruks kan dokumenteres samlet for slike hus i avtaleoversikten. Andre juridiske enheter, formål eller aktiviteter omfattes ikke automatisk fordi husene er tilknyttet hverandre eller har samme betaler.

4. Leverandørens plikter

Leverandøren skal bare behandle opplysningene etter dokumenterte instrukser, også ved overføring til tredjeland. Dersom bindende EØS-rett eller norsk rett krever annen behandling, skal Kunden informeres før behandlingen, med mindre slik informasjon er forbudt av hensyn til viktige samfunnsinteresser.

Leverandøren skal tilby opplasting, publisering og versjonshåndtering av Kundens personvernerklæring og vise den sammen med riktig virksomhetsnavn, organisasjonsnummer og personvernkontakt fra bestillingen eller virksomhetsprofilen. Kunden bestemmer hvilke av egne hus erklæringen gjelder. Leverandøren skal gi Kunden korrekt informasjon om tjenestens behandling, sikkerhet, lagring og leverandører, slik at Kunden kan oppfylle informasjonsplikten. Den offentlige leverandøroversikten skal lenkes fra husets personvernside. Publisering er ikke juridisk godkjenning av Kundens erklæring.
Før deltakerimport, utsending av invitasjoner eller aktivering av deltakermedlemskap skal løsningen kreve identifisert ansvarlig virksomhet, gyldig personvernkontakt og publisert erklæring for huset. Informasjonen skal kunne leses før innlogging gjennom sikker invitasjonstilgang der huset er privat, følge invitasjonskanalene og være tilgjengelig under «Personvern» på web og i appen. Ved innmelding skal løsningen registrere mottaksbekreftelse knyttet til riktig bruker, hus og dokumentversjon før medlemskapet aktiveres. Bekreftelsen er ikke samtykke eller bevis for faktisk lesing. Kunden har ansvar for informasjon ved innsamling og ved opplysninger fra andre etter artikkel 13 og 14, også til personer som ikke logger inn, og for nødvendige separate samtykker. Leverandøren bistår etter punkt 8. Kravene gjelder leveransen fra første lansering og bekrefter ikke at funksjonene allerede er produksjonssatt.

Leverandøren skal straks informere Kunden dersom en instruks etter Leverandørens vurdering bryter personvernregelverket. Den berørte behandlingen skal stanses i nødvendig utstrekning mens lovligheten avklares. Leverandøren skal også varsle dersom denne ikke lenger kan oppfylle sine forpliktelser.

Kun autoriserte personer med tjenstlig behov skal få tilgang. De skal være underlagt lovbestemt eller avtalefestet taushetsplikt og få relevant opplæring. Tilgang skal trekkes tilbake når behovet opphører. Leverandøren skal føre påkrevd behandlingsprotokoll og dokumentere etterlevelse.

5. Informasjonssikkerhet

Leverandøren skal gjennomføre egnede tekniske og organisatoriske tiltak etter artikkel 32, vurdert ut fra behandlingens art, omfang, sammenheng, formål og risiko. Avtalte minimumstiltak fremgår av vedlegg B. Vesentlige endringer skal dokumenteres og skal ikke redusere det avtalte beskyttelsesnivået.

Opplysninger om politisk aktivitet og andre særlige kategorier skal gis særskilt beskyttelse. Pseudonymisering, små statistikkgrupper og private lenker skal ikke fremstilles som full anonymitet eller tilstrekkelig tilgangskontroll. Leverandøren skal kunne dokumentere avgrensning mellom kunder, hus, roller og delingsnivåer.

6. Underdatabehandlere

Kunden gir generell skriftlig godkjenning til bruk av de underdatabehandlerne som er konkret identifisert og har status «Godkjent» i den dokumenterte leverandøroversikten som inngår i vedlegg C. Oppføringer med status «Ikke godkjent» gir ingen godkjenning ved signering av denne malen. Nye eller utskiftede underdatabehandlere skal varsles skriftlig minst 30 dager før de får tilgang. Varselet skal angi juridisk enhet, oppgave, opplysninger, behandlingssteder og eventuelt overføringsgrunnlag.

Kunden kan fremme en begrunnet personverninnsigelse innen 15 dager etter varselet. Partene skal søke en løsning før endringen gjennomføres. Ved uløst innsigelse skal Leverandøren tilby en forsvarlig alternativ leveranse eller la Kunden avslutte den berørte delen uten oppsigelsesgebyr og få tilbake ubenyttet forskuddsbetaling. Hvis delen ikke kan skilles ut, gjelder dette hele leveransen. Leverandøren kan ikke omgå en innsigelse ved å gjennomføre endringen først.

Underdatabehandlere skal ved skriftlig avtale pålegges minst de samme personvernforpliktelsene som følger av denne avtalen. Leverandøren er fullt ansvarlig overfor Kunden for deres oppfyllelse og skal på forespørsel dokumentere avtalekjeden. Nødvendige utdrag kan sladdes for uvedkommende forretningsopplysninger, men ikke slik at etterlevelsen ikke kan vurderes.

7. Behandlingssteder og overføring utenfor EØS

Opplysningene skal behandles på stedene og med tilgangen angitt i vedlegg C. Dette omfatter lagring, sikkerhetskopier, feilsøking, support og annen fjernaksess. Kundens godkjenning av en leverandør gir ikke alene rett til overføring utenfor EØS.

Før overføring til en mottaker utenfor EØS skal instruks, gyldig grunnlag etter GDPR kapittel V og nødvendige vurderinger og tiltak være dokumentert. Ved bruk av en adekvansbeslutning skal mottakeren og behandlingen være omfattet av beslutningen. Ved bruk av standard personvernbestemmelser skal riktig modul, vedlegg, vurdering av mottakerlandets regler og eventuelle supplerende tiltak være på plass. En generell henvisning til «SCC» er ikke tilstrekkelig.

Leverandøren skal varsle om myndighetskrav om utlevering med mindre loven forbyr det, vurdere kravets lovlighet og begrense utlevering til det lovlig påkrevde. Ulovlig eller utilstrekkelig beskyttet overføring skal stanses. Overføringsdokumentasjonen skal være tilgjengelig for Kunden. Leverandøren skal også vedlikeholde en datert oversikt som deltakerne kan lese uten innlogging, med relevante juridiske mottakere, oppgaver, opplysningstyper, lagrings- og tilgangsland og faktisk overføringsgrunnlag. Ved artikkel 46-

garantier skal den forklare hvilke garantier som gjelder, og hvordan deltakeren får tilgang til dem eller kopi. Oversikten skal stemme med vedlegg C og lenkes fra husets personvernside. Den er faktagrunnlag for Kundens erklæring og erstatter ikke denne.

8. Rettigheter og bistand

Leverandøren skal, under hensyn til behandlingens art, bistå Kunden med egnede tekniske og organisatoriske tiltak for å besvare krav om informasjon, innsyn, retting, sletting, begrensning, dataportabilitet, protest og rettigheter knyttet til automatiserte avgjørelser. Direkte mottatte henvendelser skal videresendes uten ugrunnet opphold, og senest innen to arbeidsdager. Leverandøren skal ikke avslå eller realitetsbehandle dem på Kundens vegne uten instruks, med mindre loven krever det.

Nødvendige opplysninger og tiltak skal normalt leveres innen fem arbeidsdager etter Kundens instruks, og raskere dersom lovbestemte frister krever det. Identitetskontroll skal være forholdsmessig. Eksport skal ikke gi innsyn i andres beskyttede opplysninger eller bryte avtalte regler for skjulte svar.
Leverandøren skal bistå Kunden med pliktene etter artikkel 32–36, herunder risikoanalyse, DPIA, sikkerhetshendelser og forhåndsdrøfting. Ordinær dokumentasjon, håndtering av egne avvik og nødvendig bistand som følger av feil hos Leverandøren, inngår i vederlaget. Annet omfattende tilleggsarbeid kan prises etter skriftlig forhåndsavtale. Uenighet om betaling skal ikke forsinke lovpålagte tiltak.

9. Brudd på personopplysningssikkerheten

Leverandøren skal varsle Kunden uten ugrunnet opphold etter å ha blitt kjent med et brudd, og senest innen 24 timer, også når ikke alle opplysninger er kjent. Dette er en kontraktsfrist og erstatter ikke kravet om varsling uten ugrunnet opphold. Kunden skal få løpende oppdateringer.

Varselet skal, så langt opplysningene foreligger, beskrive hendelsen, tidspunkt, berørte systemer og hus, kategorier og anslått antall registrerte og opplysningsposter, mulige konsekvenser, tiltak og kontaktperson. Leverandøren skal sikre relevante spor, begrense skade, rette årsaken og gi en skriftlig hendelsesrapport. Tiltak og bevaring av spor skal være forholdsmessige.

Kunden vurderer melding til Datatilsynet innen 72 timer når vilkårene i artikkel 33 er oppfylt, og underretning til berørte uten ugrunnet opphold ved høy risiko etter artikkel 34. Leverandøren bistår og skal ikke uttale seg på Kundens vegne uten instruks eller lovpålagt plikt. Leverandørens selvstendige lovplikter gjelder fortsatt.

10. Kontroll og revisjon

Leverandøren skal gjøre tilgjengelig all informasjon som er nødvendig for å påvise etterlevelse av artikkel 28, og muliggjøre og bidra til revisjoner og inspeksjoner fra Kunden eller en kvalifisert revisor utpekt av Kunden. Dokumentgjennomgang kan brukes først når dette er egnet; den utelukker ikke nødvendig inspeksjon.

Ordinær revisjon varsles normalt 15 arbeidsdager før og gjennomføres med rimelig hensyn til sikkerhet, drift og andre kunders opplysninger. Kortere varsel kan brukes ved hendelser, begrunnet mistanke eller myndighetskrav. Det gjelder ingen absolutt grense på én revisjon i året. Avdekkede vesentlige mangler skal rettes uten ugrunnet opphold etter en dokumentert plan. Tilsynsmyndighetenes rettigheter begrenses ikke.

11. Tilbakelevering og sletting

Ved opphør velger Kunden tilbakelevering med etterfølgende sletting eller direkte sletting. Hvis Kunden ikke gir annen instruks, er tilbakelevering med etterfølgende sletting valgt. Formater, frister, innhold, sikker overføring og eventuelle arkivkrav fremgår av vedlegg D. Leverandøren skal slette egne og underdatabehandlernes kopier, med mindre bindende EØS-rett eller norsk rett krever oppbevaring. Eventuell lovpålagt bevaring skal avgrenses, begrunnes, sikres og meddeles Kunden med hjemmel og varighet. Opplysningene skal ikke brukes til andre formål.

Et slettemerke eller avsluttet brukertilgang er ikke tilstrekkelig dokumentasjon på sletting. Sikkerhetskopier skal utgå etter den konkrete fristen i vedlegg D. De skal være avskåret fra ordinær bruk i mellomtiden; ved gjenoppretting skal slettinger gjentas før ordinær tilgang åpnes. Leverandøren skal gi skriftlig bekreftelse på gjennomført sletting, herunder når siste sikkerhetskopi er håndtert.

12. Mislighold og ansvar

Kunden kan kreve umiddelbar begrensning av ulovlig eller uforsvarlig behandling og heve den berørte leveransen ved vesentlig mislighold eller når Leverandøren ikke lenger gir tilstrekkelige garantier. Forsvarlig tilbakelevering og sletting skal ivaretas også ved tvist. Partenes innbyrdes økonomiske ansvar reguleres av hovedavtalen så langt loven tillater det. Avtalen begrenser ikke registrertes rettigheter eller krav etter artikkel 82, myndighetenes kompetanse eller partenes lovpålagte ansvar. Norsk rett gjelder, med tvisteløsning som avtalt i hovedavtalen.

Vedlegg A – Behandlingen og instruksen

Instruksen gjelder Kundens hus identifisert i bestillingen eller den tilhørende avtaleoversikten. Denne skal angi den juridiske behandlingsansvarlige, eventuell rolle som databehandler og hvilke av aktivitetene nedenfor Kunden har bestilt. Samme ansvarlige og samme avtalte bruk kan dokumenteres samlet for flere hus. Ved deling mellom selvstendige enheter skal ansvar, formål, mottakere og nødvendig avtale om delingen fremgå. Tilknytning i et hustre oppretter ikke i seg selv en lovlig delingsordning.

Registrerte er de ansatte, medlemmer, tillitsvalgte, frivillige, kontaktpersoner, innbyggere, inviterte og arrangementdeltakere som omfattes av Kundens valgte bruk. Bestillingen identifiserer de aktuelle gruppene, forventet omfang og eventuell særlig sårbarhet. Standardleveransen er avgrenset til personer som har fylt 18 år. Behandling for yngre personer krever særskilt avtalt tilgangsordning, tilpasset informasjon og nødvendig rettslig grunnlag. Tabellen avgrenser hvilke opplysninger hver aktivitet kan omfatte. Bestillingens konkrete bruk og dokumenterte lagringsplan bestemmer hvilke aktiviteter og felter som faktisk tas i bruk. Teknisk tilgjengelige funksjoner er ikke dermed bestilt.

Aktivitet	Opplysninger og behandling	Tillatt bruk og tilgang
Medlems- og rolleadministrasjon	Navn, konto-ID, kontaktopplysninger, hus, rolle, invitasjon og medlemsstatus; registrere, oppdatere og kontrollere tilgang	Administrere deltakelse, tilgang og roller i Kundens hus. Tilgang for autoriserte administratorer og avtalte deltakergrupper; kontaktvisning bare innenfor den avtalte innstillingen.
Avstemninger og undersøkelser	Spørsmål, svar, pseudonyme identifikatorer, tidspunkter, hus, eventuelt navn ved åpne svar eller deltakerliste	Gjennomføre Kundens avtalte medvirkning og behandle resultatene. Bestillingen angir sakstyper og hvilke deltakergrupper som omfattes. Åpne

		svar og navngitte deltakerlister krever særskilt avtalt synlighet og informasjon før deltakelse.
Ideer, problemer og kommentarer	Tekst, navn, profilbilde, vedlegg og eventuell husangivelse; lagre, vise og moderere	Ta imot, drøfte og følge opp innspill innenfor valgt bruk. Synlighet følger den avtalte deltakerkretsen; tilgang oppover eller på tvers av hus må være omfattet av avtaleoversikten.
Arrangementer og kunngjøringer	Påmelding, kapasitet, kommentarer, navn, hus og eventuelle kontaktfelt	Informere deltakere og administrere påmelding og gjennomføring. Arrangør, kontaktvisning og deltakernes innsyn følger valgt bruk; delte deltakerlister krever dokumentert avgrensning.
Dokumenter og media	Filinnhold, navn på opplaster, filmetadata og tilgangsinnstillinger	Dele dokumenter og media til den avtalte kretsen. Kunden begrenser innholdet til det som er nødvendig for formålet. Tilgang til private filer skal kontrolleres.
Demografi og resultater	Alder, kjønn, bostedskommune og stemmesvar der funksjonen brukes; deretter gruppere og vise resultater	Bare når demografisk resultatvisning er bestilt og har dokumentert grunnlag. Leverandøren dokumenterer terskler, koblingsrisiko og tilgang. Det skal ikke gis løfte om anonymitet uten dokumentert vurdering av det faktiske datasettet.
Fravær og andre personalmoduler	Dato, fraværstype, eventuell helseopplysning, merknad og godkjenner	Ikke omfattet av standardbruk. Krever særskilt avtalt nødvendighet, formål, konkrete data, artikkel 6-grunnlag, eventuelt artikkel 9-unntak, avgrenset tilgang og sletting.
Arbeidstid, hvis særskilt avtalt	Inn-/utstempling, person, hus, tidspunkt, korrigeringer og hvem som endret	Ikke omfattet av standardbruk. Krever særskilt avtalt formål, artikkel 6-grunnlag, tilgang, nødvendig drøfting og lagringsplan.
KI-bistand	Valgt tekst og kategorier oversendes godkjent KI-leverandør for avtalt analyse eller utkast	Bare etter særskilt bestilt KI-oppgave og godkjenning etter vedlegg C. Instruksen skal angi hvilke tekster som kan sendes. Opplysningene skal begrenses til det nødvendige. Kundens innhold skal ikke brukes til modelltrening. Særlige kategorier og fortrolig innhold krever uttrykkelig avtalt grunnlag og beskyttelse før oversending.
Personverninformasjon og mottaksbekreftelser	Kundens PDF-er og versjoner, publiseringsdato og administrator; mottaksbekreftelse med bruker, hus, tidspunkt, dokumentversjon og referanse til viste virksomhets- og kontaktopplysninger; midlertidig kobling til invitasjonen før innlogging	Publisere og vise Kundens informasjon, formidle invitasjoner og dokumentere mottaksbekreftelse ved innmelding. Tilgang avgrenses til riktig hus og virksomhet. Midlertidige bekreftelser, dokumenthistorikk og kvitteringer følger lagringsplanen i vedlegg D og er ikke samtykkeregister eller bevis for faktisk lesing.
Drift og bistand	Kundespesifikke logger, feilopplysninger, eksport, gjenoppretting og sletting	Bare nødvendig drift og oppfyllelse av denne avtalen innenfor aktivitetene i A, tiltakene i B, leverandørene i C og fristene i D

Særlige kategorier omfattes bare når bestillingen identifiserer kategorien og formålet, og Kunden har dokumentert grunnlag etter artikkel 6 og et anvendelig unntak etter artikkel 9. Kunden skal gi deltakerne den påkrevde informasjonen. Opplysninger om straffedommer og lovovertredelser krever særskilt grunnlag etter artikkel 10 og avtalt sikkerhet. Pasientjournaler og taushetsbelagte kommunale enkeltsaker er ikke del av standardleveransen.
Tilgang gis til Kundens autoriserte administratorer og de deltakergruppene Kunden har valgt for aktiviteten. Avtaleoversikten skal synliggjøre eventuell arvet administratortilgang, tilgang til ideer og problemer oppover i hustreet, resultater for små grupper, felles kommentartråder og visning av navn eller hus i deltakerlister. Deling utenfor den avtalte deltakerkretsen krever uttrykkelig instruks. Kunden skal gi deltakerne tilsvarende informasjon i sin erklæring og før den aktuelle delingen eller avstemningen. Leverandøren bistår med opplysninger om faktisk tilgang og synlighet.

Stemmesvar i alle hemmelige avstemninger skal pseudonymiseres. Det betyr at navnet erstattes med en identifikator; svarene er fortsatt personopplysninger. Skjulte svar skal ikke knyttes til navn i ordinær kunderapportering. Leverandøren skal dokumentere konkrete tiltak

mot identifisering gjennom små grupper, demografi og sammenstilling. Kunden skal ikke kombinere lister, resultater eller andre datasett for å avdekke skjulte individuelle svar. En minstestørrelse i én rapport er ikke en generell anonymitetsgaranti. Leverandøren skal ikke rekonstruere koblinger for ordinær kunderapportering. Pseudonymisering endrer ikke kravene til behandlingsgrunnlag, lagringsbegrensning og sletting etter vedlegg D.

Vedlegg B – Avtalte sikkerhetstiltak

Tabellen fastsetter avtalte minimumstiltak som skal være dokumentert før produksjonsbruk og opprettholdes under avtalen. Leverandøren holder dokumentasjonen oppdatert og gjør relevant dokumentasjon tilgjengelig for Kunden etter punkt 10. Kunden trenger ikke beskrive Leverandørens tekniske drift. Bestillingen kan fastsette mer konkrete sikkerhets- og kontinuitetskrav ut fra Kundens bruk.

Område	**Kontraktskrav**	Leverandørens dokumentasjonsplikt
Tilgang	Personlige kontoer, rollebasert tilgang etter minste privilegium, flerfaktor for privilegert driftstilgang, løpende tilbakekalling og periodisk tilgangskontroll.	Tilgangsoversikt, kontrollhistorikk og dokumentasjon av flerfaktor for privilegert driftstilgang.
Avgrensning	Kontroller mellom kunder, hus og roller, også for eksport, API-er, arv og delte ressurser	Dokumenterte tilgangstester og håndtering av funn på tvers av hus, roller og kunder.
Filer	Private filer krever reell autorisasjon; offentlig ACL eller en vanskelig gjettbar lenke er ikke tilstrekkelig vern	Dokumenterte lagringsregler og tester av autorisasjon for private filer.
Kryptering	AES-256-kryptering i hvile og TLS 1.3 under overføring, med kontrollert tilgang til og håndtering av krypteringsnøkler.	Oversikt over krypteringens omfang, protokoller, nøkkeltilgang og nøkkelhåndtering.
Stemmer	Pseudonymisering av hemmelige stemmesvar og begrenset tilgang til koblingsdata. Sletting eller særskilt avtalt anonymisering følger planen i vedlegg D. Navngitte svar og deltakerlister skal bare brukes innenfor uttrykkelig avtalt synlighet.	Beskrivelse av koblingsdata, tilganger, slette- eller avtalt anonymiseringsmetode, tidsstyring og kontroll av resultatet.
Logging	Sporbar privilegert tilgang og sikkerhetshendelser; ikke unødvendige innholdsdata eller hemmeligheter i logger	Oversikt over loggtyper, formål, tilganger og sletterutine i samsvar med vedlegg D.
Sikker drift	Oppdateringer, sårbarhetshåndtering, endringskontroll, regelmessige sikkerhetsrevisjoner og penetrasjonstester samt dokumentert hendelsesrutine.	Rutiner og historikk for sikkerhetsoppdateringer, sårbarheter, testing og hendelseshåndtering.
Kontinuitet	Sikrede sikkerhetskopier og dokumentert, testet gjenoppretting.	Backup- og gjenopprettingsrutine, testresultater og eventuelle gjenopprettingsmål avtalt i hovedavtalen.
Utvikling og støtte	Atskilt testmiljø; produksjonsdata bare ved dokumentert behov og egnede tiltak; autorisert supporttilgang	Rutiner for testdata, autorisert supporttilgang og dokumenterte land for eventuell ekstern tilgang.
Sletting	Dekker databasekoblinger, filer, søkeindekser, logger der relevant og underleverandører	Dokumenterte slettetester, oversikt over kopier og bekreftelser fra underdatabehandlere.
Organisasjon	Taushetsplikt, opplæring, risikovurdering, årlig internrevisjon og DPIA samt løpende vurdering ved endringer som påvirker risikoen.	Taushetsforpliktelser, opplæring, oppdatert risiko- og personvernkonsekvensvurdering samt rapporter fra internrevisjon og oppfølging av tiltak.

Vedlegg C – Underdatabehandlere og behandlingssteder

Tabellen identifiserer aktuelle tjenester og avgrenser hvilke oppgaver de kan utføre. Leverandøren skal før de får tilgang til Kundens opplysninger knytte hver tjeneste til en dokumentert, datert leverandøroversikt med riktig juridisk avtalepart, oppgave,

opplysningskategorier, lagrings- og tilgangsland, videre leverandørkjede, lagringstid, databehandleravtale og faktisk overføringsgrunnlag der det foreligger en overføring. Denne oversikten inngår i vedlegg C og angir godkjenningsstatus. Uavklarte oppføringer er ikke godkjent ved denne malen; en produktbetegnelse eller en generell SCC-henvisning erstatter ikke opplysningene. Deltakernes oversikt etter punkt 7 skal vise den samme faktiske behandlingen uten å forutsette tilgang til avtalen. Senere endringer behandles etter punkt 6 og 7. Oversikt i dokumentpakken: Leverandører og overføringer

Tjeneste / leverandør	**Oppgave og data**	Krav til leverandøroversikten	Godkjenningsstatus
Amazon Web Services (AWS)	Infrastruktur, lagring, database-/filbehandling og sikkerhetskopier for de AWS-tjenestene som faktisk brukes.	Juridisk avtalepart og konkrete produkter; land for lagring, sikkerhetskopier og tilgang; avtalekjede, lagringstider og eventuelle overføringsgrunnlag.	Ikke godkjent ved denne malen. Godkjenning forutsetter dokumentert oppføring etter punkt 6 og 7.
Google LLC / Firebase Cloud Messaging	Push-token, varseltekst og nødvendig datapayload for utsending av pushvarsler. Skilles fra Google Play-kjøp.	Standardpart Google LLC; global behandling inkludert USA; DPF og subsidiære SCC etter avtalen, nærmere beskrevet i dokument 10. Dokumenter tjenesteomfang, eventuelle særvilkår, dataminimering, slettingskall og meldingslevetid.	Ikke godkjent ved denne malen. Godkjenning forutsetter dokumentert oppføring etter punkt 6 og 7.
Domeneshop AS	E-post med mottakeradresse, invitasjoner, varsler og nødvendig meldingsinnhold.	E-postservere i Norge etter leverandørens produktside; databehandleravtale i tillegg 3. Avgrens faktisk e-post-/support-/backupkjede og frister; øvrige tjenester i Domeneshops leverandørliste inngår ikke automatisk.	Ikke godkjent ved denne malen. Godkjenning forutsetter dokumentert oppføring etter punkt 6 og 7.
Anthropic Ireland, Limited / Claude API	Bare særskilt avtalt KI-bistand: sakstittel, beskrivelse og kategorier som Kunden instruerer Leverandøren om å analysere.	Standardpart i Irland, USA-lagring og SCC modul 2/3 er dokumentert i offentlige vilkår. Avklar arbeidsområdets geografi, eventuell nullagring/særavtale og avtaledekning for særlige kategorier. Bruk og lagring må følge den konkrete instruksen og dokument 10.	Ikke godkjent ved denne malen. Krever i tillegg særskilt instruks etter vedlegg A; funksjonen skal ikke sende Kundens data før kravene er oppfylt.
Eksterne utviklings-, support- eller driftsleverandører	Eventuell tilgang ved vedlikehold eller bistand.	Hver juridiske enhet og oppgave skal identifiseres enkeltvis, med tilgangsland, opplysninger, lagringstid, avtale og overføringsgrunnlag.	Ingen slike leverandører er godkjent gjennom denne generelle kategorien.

Vipps brukes til kontoinnlogging. Signicat/BankID gjelder tidligere identifikasjon og er ikke del av ordinær ny innlogging. Vipps, Apple, Google Play, Stripe og Fiken omfattes ikke automatisk av Kundens underdatabehandlergodkjenning når de behandler opplysninger for personlig konto, egne kjøp eller Leverandørens fakturering. Slik behandling og de faktiske rollene beskrives i Leverandørens personvernerklæringer (dokument 04 og 05). Dersom en av disse tjenestene skal behandle Kundens husdata på instruks, kreves særskilt oppføring og godkjenning etter dette vedlegget. AWS sin oversikt over egne underleverandører er bare én del av kjeden og erstatter ikke Leverandørens samlede oversikt.

Vedlegg D – Frister, opphør og instruksjonskanaler

Fristene nedenfor gjelder behandling på Kundens vegne. Hovedavtalens avtaleoversikt skal inneholde eller identifisere en vedlagt, avtalt lagringsplan med konkrete frister eller klare slettekriterier og utløsende hendelse for hver aktivitet. Dette omfatter også pseudonymiserte stemmesvar og tilhørende koblings- og deltakelsesopplysninger. Leverandøren skal

dokumentere hvilke slettefunksjoner og frister tjenesten kan oppfylle, og gjennomføre den avtalte instruksen. Kunden skal gi tilsvarende informasjon i sin erklæring. Behandling av en aktivitet starter først når frister og metoder er dokumentert og kan gjennomføres. Opplasting av en erklæring endrer ikke lagringsinnstillinger eller gir i seg selv instruks om sletting eller anonymisering.

Punkt	Avtalt ordning
Autoriserte instruksjonsgivere	Kundens avtalerepresentant og personer som representanten skriftlig har gitt fullmakt. Fullmakter og avtalte skriftlige kanaler registreres i avtaleoversikten. Rutinemessige valg kan gjøres av autoriserte administratorer innenfor bestillingen.
Lagring under avtalen	Stemmesvar i alle hemmelige avstemninger pseudonymiseres og er fortsatt personopplysninger. Lagringsplanen i hovedavtalens avtaleoversikt skal angi frist eller konkret slettekriterium og når fristen begynner å løpe, for stemmesvar, koblingsopplysninger og deltakelsesopplysninger. Planen skal også dekke invitasjoner og midlertidige bekreftelser før innlogging, medlemskap, innhold, deltakerlister, publiserte personverndokumenter, versjonshistorikk, mottaksbekreftelser og utmelding. Dokumenthistorikk og bekreftelser oppbevares bare etter et dokumentert formål og den avtalte fristen eller slettekriteriet. «Så lenge nødvendig» alene er ikke et konkret kriterium. Pseudonymisering gir ikke rett til ubegrenset lagring. Kunden informerer deltakerne i sin erklæring; Leverandøren gjennomfører den avtalte planen. Opplasting av et dokument endrer ikke instruksen eller de tekniske innstillingene.
Valg ved opphør	Tilbakelevering og deretter sletting, med mindre Kunden skriftlig velger direkte sletting.
Eksport	Leverandøren tilbakeleverer Kundens opplysninger, tilhørende filer og nødvendige metadata gjennom sikker overføring til Kundens avtalerepresentant eller skriftlig utpekte mottaker. Maskinlesbart format og eventuelle arkivkrav fastsettes i bestillingen ut fra de aktuelle dataene; eksporten skal ikke avhenge av at Kunden fortsetter abonnementet.
Frist for eksport	Innen 30 dager etter opphør eller instruks; kortere ved nødvendige lovfrister.
Frist for aktive kopier	Innen 30 dager etter tilbakelevering eller instruks om direkte sletting, og senest 60 dager etter opphør med mindre en konkret lovlig overgangsperiode er skriftlig avtalt. Manglende mottaksbekreftelse fra Kunden utsetter ikke fristen ubestemt; Leverandøren varsler og dokumenterer sikker levering.
Sikkerhetskopier hos Leverandøren	Opplysninger som er slettet fra aktive systemer, skal være slettet eller overskrevet i Leverandørens sikkerhetskopier senest 14 dager senere. Kopiene skal ikke brukes ordinært i mellomtiden. Ved gjenoppretting skal tidligere slettinger gjennomføres før ordinær tilgang åpnes. Eksterne leverandørers egne kopier og lagringstider skal være dokumentert i vedlegg C; denne fristen er ikke en bekreftelse på deres praksis.
Løpende sletting og rettighetskrav	Punkt 8 gjelder; opphørsfristene utsetter ikke rettigheter under avtalen.
Lovpålagt bevaring	Særskilte lovpålagte bevaringskrav skal identifiseres med hjemmel, datakategori, formål og frist i avtaleoversikten. For Leverandørens egen lovpålagte bevaring gjelder punkt 11. En generell arkivreservasjon gir ingen rett til ubegrenset oppbevaring.
Slettebekreftelse	Sendes Kundens avtalerepresentant eller skriftlig utpekte mottaker, med dato, omfang, berørte underdatabehandlere og tidspunkt for håndtering av siste sikkerhetskopi.
Særkrav for kommune, politisk parti eller andre	Bare særkrav som fremgår konkret av bestillingen eller et avtalt tillegg, gjelder. Dette kan omfatte arkivoverføring, separasjon, behandlingssted, DPIA-bistand og særskilte instrukser.
Sikkerhetslogger hos Leverandøren	Ordinære sikkerhetslogger oppbevares i 14 dager fra registreringen. Ved en konkret sikkerhetshendelse kan nødvendige, avgrensede spor bevares særskilt så lenge dokumentert håndtering eller rettslig krav gjør det nødvendig. Formål, tilgang og ny slettefrist skal da dokumenteres. Fristen omfatter ikke automatisk innholdsdata, personverndokumenter, mottaksbekreftelser, revisjonsspor som Kunden uttrykkelig har bestilt, eller eksterne leverandørers egne logger.
Henvendelser og kundestøtte	Kundespesifikt innhold i support behandles bare når det er nødvendig for bistanden og etter Kundens dokumenterte lagringsplan. Leverandørens egne kontakt- og supportopplysninger behandles for egne formål etter personvernerklæringene i dokument 04 og 05. Fristene på 12 måneder for ordinære henvendelser og 24 måneder for support gir ikke adgang til å beholde kopier av Kundens husinnhold utover instruksen.