Personvern ved kapitalbekreftelse

Vedlegg til oppdragsavtalen for kapitalbekreftelse.no | Versjon 1.0

Denne erklæringen forklarer hvordan Amicus AS behandler personopplysninger når du besøker kapitalbekreftelse.no, kontakter oss, ber om pristilbud eller bestiller bekreftelse av innbetalt aksjekapital. Den omfatter også tilbudslenker, tilbudskoder og bekreftelse av e-postadresse. Erklæringen gjelder dessuten personer som omtales i dokumentasjonen vi mottar, blant annet stiftere, aksjeeiere, reelle rettighetshavere og representanter for kunden.

1 Hvem som er ansvarlig

Amicus AS, organisasjonsnummer 930 792 977, er behandlingsansvarlig for personopplysningene vi behandler for å besvare henvendelser, utarbeide tilbud, vurdere og utføre kapitalbekreftelsesoppdraget, gjennomføre lovpålagt kundekontroll og administrere vårt eget kundeforhold. Kapitalbekreftelse.no er en tjeneste levert av Amicus AS.

Du kan kontakte oss om personvern og dine rettigheter på post@amicus.as, telefon +47 92 30 66 25 eller per post til Radka Toneffs vei 20A, 1410 Kolbotn.

Ved kapitalbekreftelsen gjør vi en selvstendig faglig kontroll. Dette vedlegget gir informasjon om vår behandling av personopplysninger og er ikke en databehandleravtale med kunden. Eventuelle andre tjenester, som bokføring og lønn, vurderes og reguleres særskilt.

2 Hvilke opplysninger vi behandler

Avhengig av oppdraget behandler vi navn, kontaktopplysninger, rolle, fullmakter, signatur, eierandel og opplysninger om eierskap og kontroll. Fødselsdato, fødselsnummer eller D-nummer og legitimasjonsopplysninger behandles når det er nødvendig for sikker identifisering eller lovpålagt kundekontroll.

Vi behandler dokumentasjon om kapitalinnskuddet, blant annet beløp, dato, innbetaler, relevante kontoopplysninger, bankens bekreftelse, stiftelsesdokument, vedtekter og eventuelle dokumenter om kapitalforhøyelse. Vi behandler også bestillingsopplysninger, relevant korrespondanse, betalingsstatus, fakturaopplysninger og vår dokumentasjon av kontrollen.

Ved prisforespørsler og tilbud behandler vi opplysninger om selskapet, sakstype, antall tegnere, kontaktperson, e-post, telefon og eventuelle kommentarer. Vi registrerer tilbudspris, gyldighet, tilbudsversjon og hendelser som utsending, bekreftelse av tilbudsprisen og videreføring til bestilling. Når du bruker tilbudslenke, tilbudskode eller engangskode fra e-post, behandler vi nødvendige opplysninger om tilgang, verifikasjon og bruk av løsningen.

Kundekontrollen kan omfatte midlenes opprinnelse, politisk eksponert stilling (PEP), relevante sanksjoner og nødvendige risikovurderinger. Vi samler bare inn opplysninger som er nødvendige for formålet. Eventuelle opplysninger omfattet av GDPR artikkel 9 eller 10 behandles bare når det finnes særskilt rettslig grunnlag, blant annet hvitvaskingsforskriften § 6-1 når vilkårene er oppfylt.

3 Hvor opplysningene kommer fra

Opplysningene kommer fra deg, selskapet eller personer som representerer det, fra innsendte dokumenter, banken og relevante offentlige registre, som Brønnøysundregistrene og registeret over reelle rettighetshavere. Ved behov bruker vi relevante kilder for identitetskontroll, PEP- og sanksjonskontroll og åpne kilder som er nødvendige for kundekontrollen. Du kan spørre oss hvilke kilder vi har brukt om deg, med de begrensningene som følger av lov.

4 Formål og rettslig grunnlag

Vi bruker personopplysninger til følgende formål. Behandlingsgrunnlaget vurderes for den enkelte behandlingen og personen opplysningene gjelder.

Formål	Rettslig grunnlag
Prisforespørsler og tilbud	GDPR art. 6 nr. 1 bokstav f. Vi og kunden har en berettiget interesse i å besvare forespørsler, avtale pris og følge opp tilbud. Bokstav b brukes når behandlingen gjelder tiltak før avtale med den registrerte selv.
Bestilling, kontakt og kapitalbekreftelse	GDPR art. 6 nr. 1 bokstav f. Vår og kundens berettigede interesse er å få utført og dokumentert en forsvarlig kontroll av innbetalt kapital og kommunisere om oppdraget. Bokstav b brukes bare når behandlingen er nødvendig for en avtale med den registrerte selv eller tiltak før slik avtale.
Kundekontroll og tiltak mot hvitvasking	GDPR art. 6 nr. 1 bokstav c, jf. hvitvaskingsloven, særlig §§ 9-15, 17-18, 24-26 og 30-32. Vi må blant annet identifisere kunden og relevante personer, vurdere risiko og oppbevare nødvendig dokumentasjon.
Fakturering og eget regnskap	GDPR art. 6 nr. 1 bokstav c for lovpålagt bokføring og oppbevaring, jf. bokføringsloven §§ 10 og 13. Nødvendig administrasjon av kontaktpersoner bygger på bokstav f.
Sikkerhet og dokumentasjon av rettskrav	GDPR art. 6 nr. 1 bokstav f. Vi har en berettiget interesse i å bekrefte tilgang til riktig sak, beskytte tjenesten mot misbruk og dokumentere, gjøre gjeldende eller forsvare rettskrav. Vi begrenser behandlingen til det som er nødvendig.
Valgfri sporing og markedsføring	GDPR art. 6 nr. 1 bokstav a når samtykke kreves. Samtykke til eventuell markedsføring eller valgfri sporing innhentes separat. Se punkt 11.

Når vi bruker berettiget interesse, veier vi behovet for behandlingen mot ditt personvern. Vi begrenser opplysningene og tilgangen, og bruker dem bare til relevante formål. Du kan protestere på denne behandlingen, se punkt 10.

5 Opplysninger vi trenger for å utføre oppdraget

Vi kan ikke gjennomføre oppdraget dersom vi mangler nødvendig dokumentasjon av kapitalinnskuddet eller ikke kan oppfylle kundekontrollen. Vi opplyser om hvilke opplysninger som er nødvendige når vi ber om dem. Opplysninger til valgfrie formål er frivillige.

For å behandle en prisforespørsel trenger vi kontaktopplysninger og tilstrekkelige opplysninger om den ønskede tjenesten. En prisforespørsel utløser ikke i seg selv full kundekontroll. Opplysninger som er nødvendige for kundekontroll og kapitalbekreftelse, innhentes når oppdraget skal vurderes og gjennomføres. Tilbuds- og statusmeldinger gjelder saken din og innebærer ikke påmelding til markedsføring.

At kunden inngår avtale med oss, innebærer ikke at alle aksjeeiere, styremedlemmer eller andre personer er parter i avtalen. Vi bruker derfor ikke avtale som et generelt behandlingsgrunnlag for alle personer i dokumentasjonen.

6 Sikker innsending og tilgang

Bruk løsningen vi anviser for sikker innsending av legitimasjon, fødselsnummer og bankdokumentasjon. Ikke send slike dokumenter i vanlig, ukryptert e-post. Unngå opplysninger om andre transaksjoner eller personer som ikke er relevante. Avklar eventuell sladding med oss dersom den kan påvirke kontrollgrunnlaget.

Tilbudslenker og tilbudskoder brukes til å finne riktig tilbud og gjenoppta den lagrede saken. Vi kan be deg bekrefte e-postadressen med en engangskode før du får tilgang. E-postbekreftelsen beskytter tilgangen til saken og erstatter ikke BankID-identifisering eller annen lovpålagt kundekontroll. Ikke del tilgangslenker eller koder med uvedkommende.

Vi skal beskytte opplysningene med egnede tekniske og organisatoriske tiltak. Tilgang begrenses til personer med tjenstlig behov og underlagt taushetsplikt eller annen bindende konfidensialitetsplikt.

7 Hvem opplysningene kan deles med

Vi deler bare opplysninger når det er nødvendig, det finnes behandlingsgrunnlag og delingen er forenlig med taushetsplikten. Dette kan omfatte banken for å kontrollere innbetalingen, kunden og kundens autoriserte representanter, og Brønnøysundregistrene gjennom Altinn når bekreftelsen inngår i registreringsmeldingen. Vi gir ikke andre aksjeeiere automatisk tilgang til legitimasjon eller fullstendig kundekontrolldokumentasjon.

Vi bruker underleverandører til drift og gjennomføring av tjenesten. De får bare opplysninger som er nødvendige for sine oppgaver:

Signant leverer kundekontrollskjema og BankID-identifisering og behandler nødvendige identitets-, eier- og kundekontrollopplysninger.

Stripe leverer kortbetaling og behandler nødvendige betalings- og transaksjonsopplysninger. Stripe kan være databehandler for enkelte oppgaver og selvstendig behandlingsansvarlig for andre, blant annet egne lovpålagte kontroller og tiltak mot svindel.

Der en underleverandør behandler personopplysninger på våre vegne, skal behandlingen være regulert av databehandleravtale. Banker, offentlige myndigheter og enkelte leverandører kan være selvstendig behandlingsansvarlige for sin behandling.

Finanstilsynet, Økokrim og andre offentlige myndigheter kan motta opplysninger når vi har plikt eller lovlig adgang til å gi dem. Ved nødvendig håndtering av rettskrav kan opplysninger deles med advokat eller forsikringsselskap innenfor rammene av taushetsplikten.

8 Lagringssted og overføring utenfor EØS

Underleverandørenes behandling kan innebære overføring til land utenfor EØS eller fjernaksess fra slike land. Stripe beskriver internasjonal behandling, blant annet i USA og India. Når vår bruk av en leverandør innebærer en slik overføring, skal den ha et gyldig overføringsgrunnlag etter GDPR kapittel V. Aktuelle grunnlag er en beslutning om tilstrekkelig beskyttelsesnivå eller EUs standard personvernbestemmelser med nødvendige tilleggstiltak. Du kan kontakte oss for informasjon om hvilke overføringer og garantier som gjelder for opplysningene dine, og hvordan du får et eksemplar av garantiene.

9 Hvor lenge vi oppbevarer opplysningene

Dokumentasjon etter hvitvaskingsregelverket oppbevares som hovedregel i fem år etter at kundeforholdet er avsluttet eller den enkeltstående transaksjonen er gjennomført. Fristen er ti år når kundeforholdet ved avslutning var underlagt forsterkede kundetiltak, eller transaksjonen var underlagt slike tiltak, jf. hvitvaskingsforskriften § 6-4. Etter fem år kan vi vurdere sletting dersom særlige grunner tilsier at kunden likevel ikke utgjorde høy risiko. En slik vurdering dokumenteres og oppbevares i ytterligere fem år. Lovens regler om sletting og eventuelle unntak gjelder.

Kapitalbekreftelsen og nødvendig dokumentasjon av vår kontroll oppbevares som hovedregel i fem år etter utløpet av året oppdraget ble avsluttet, for å dokumentere arbeidet og kunne håndtere rettskrav. Oppbevaring som er lovpålagt bygger på GDPR art. 6 nr. 1 bokstav c; annen nødvendig oppbevaring bygger på bokstav f. Dette gir ikke adgang til å beholde kundekontrollopplysninger utover hvitvaskingsregelverkets frister.

Opplysninger som inngår i vårt oppbevaringspliktige regnskapsmateriale, lagres normalt i fem år etter regnskapsårets slutt. Andre lovpålagte frister følges der de gjelder.

Ordinære henvendelser, prisforespørsler, tilbud som ikke fører til oppdrag, og ufullførte bestillinger uten særskilt oppbevaringsplikt slettes senest 90 dager etter siste kontakt eller aktivitet. En prisforespørsel får ikke automatisk fem eller ti års lagringstid etter hvitvaskingsregelverket. Tilbud og prisbekreftelser som inngår i en bestilling eller et oppdrag, oppbevares sammen med relevant avtale-, oppdrags- eller regnskapsdokumentasjon etter fristene som gjelder for dette materialet.

Tilbudslenker og tilbudskoder deaktiveres når de ikke lenger skal gi tilgang til et aktivt tilbud eller en pågående bestilling. Engangskoder for e-post har kort gyldighet og slettes når de er brukt eller utløpt. Tekniske tilgangs- og sikkerhetslogger slettes eller anonymiseres senest etter 90 dager, med mindre en konkret sikkerhetshendelse gjør lengre lagring nødvendig. Nødvendig historikk om selve tilbudet eller bestillingen følger fristene for saken.

Etter fristene slettes eller anonymiseres opplysningene. Nødvendig dokumentasjon knyttet til en konkret tvist kan oppbevares så lenge tvisten eller rettskravet krever det, innenfor ufravikelige slettefrister. Sikkerhetskopier fases ut etter fastsatt omløpstid og skal ikke brukes som et varig arkiv.

10 Dine rettigheter

Du kan be om innsyn i personopplysningene vi har om deg og om å få uriktige opplysninger rettet. Når vilkårene er oppfylt, kan du be om sletting, begrensning av behandlingen og dataportabilitet. Dataportabilitet gjelder ved automatisert behandling som bygger på samtykke eller avtale med deg.

Du kan protestere på behandling som bygger på berettiget interesse. Da vurderer vi om det finnes tvingende berettigede grunner til å fortsette, eller om behandlingen er nødvendig for rettskrav. Ved eventuell direkte markedsføring kan du alltid protestere. Samtykker kan trekkes tilbake like enkelt som de ble gitt, uten at det påvirker lovligheten av tidligere behandling.

Sletting og innsyn kan være begrenset av lovpålagt oppbevaring, taushetsplikt og hvitvaskingsregelverket. Vi kan for eksempel være avskåret fra å opplyse om undersøkelser eller rapportering til Økokrim. Vi vurderer hvert krav konkret.

Kontakt post@amicus.as for å bruke rettighetene dine. Vi svarer uten ugrunnet opphold og normalt senest innen én måned. Dersom en lovlig fristforlengelse er nødvendig, får du beskjed innen den første måneden. Vi kan be om nødvendig og forholdsmessig bekreftelse av identiteten din.

Du kan klage til Datatilsynet. Se www.datatilsynet.no for fremgangsmåte og kontaktinformasjon. Du kan gjerne kontakte oss først, men det er ikke et vilkår for å klage.

11 Bruk av nettstedet og informasjonskapsler

Ved bruk av nettstedet kan tekniske opplysninger som IP-adresse, tidspunkt, nettleser, enhet og tekniske hendelser inngå i nødvendig drift og sikkerhet. Behandling av personopplysninger til dette formålet bygger på vår berettigede interesse i å tilby og beskytte tjenesten, jf. GDPR art. 6 nr. 1 bokstav f.

Nødvendige sesjoner og tilgangsfunksjoner kan brukes for å huske en bekreftet tilgang og la deg fortsette med riktig tilbud eller bestilling. Tilbudslenker, tilbudskoder, legitimasjonsopplysninger og dokumentinnhold skal ikke deles med tredjeparts analyse- eller markedsføringsverktøy.

Lagring av eller tilgang til informasjon på enheten din er også regulert av ekomloven § 3-15. Strengt nødvendig teknologi for en tjeneste du uttrykkelig ber om, kan være unntatt fra samtykkekravet. Annen slik teknologi krever forhåndssamtykke. Det skal være mulig å avslå og senere trekke tilbake valgfrie samtykker.

12 Automatiserte avgjørelser

Selve kapitalbekreftelsen skal bygge på en faglig vurdering. Oppdraget skal ikke avgjøres utelukkende automatisk på en måte som har rettsvirkning eller tilsvarende betydelig virkning for deg. Eventuelle automatiske treff i identitets-, PEP- eller sanksjonskontroll må vurderes før de brukes som grunnlag for en slik avgjørelse.

Automatisk prisvisning, kontroll av en tilbudskodes gyldighet og utsending av meldinger er administrative funksjoner. De erstatter ikke vår faglige vurdering eller nødvendige kundekontroll.

13 Informasjon til andre og endringer

Når vi mottar opplysninger om deg fra andre, skal vi gi deg denne informasjonen innen fristene i GDPR artikkel 14, med mindre et lovlig unntak gjelder. Vi kan be kunden videresende informasjonen, men beholder ansvaret for at informasjonsplikten blir oppfylt.

Vi oppdaterer erklæringen når tjenesten eller behandlingen endres. Vesentlige endringer formidles på en egnet måte. Erklæringen er informasjon om behandlingen; du trenger ikke samtykke til den for at vi skal oppfylle våre lovpålagte plikter.