esigner.no

Databehandleravtale

Avtale om behandling av personopplysninger etter GDPR artikkel 28

1. Partene

Behandlingsansvarlig:

Virksomhetens navn

Organisasjonsnummer

Adresse

Kontaktperson

E-post

Telefon

Databehandler:

Virksomhetens navn

Organisasjonsnummer

Adresse

Kontaktperson

E-post

Telefon

2. Avtalens formål og omfang

Avtalen regulerer databehandlers behandling av personopplysninger på vegne av behandlingsansvarlig, jf. personvernforordningen (GDPR) artikkel 28. Hovedavtalen som regulerer det underliggende leveranseforholdet er:

Hovedavtale / tjenestebeskrivelse (navn og dato)

3. Behandlingens art, formål og varighet

Behandlingen omfatter følgende:

Formålet med behandlingen

Behandlingens art (f.eks. lagring, drift, support)

Varighet (fra dato – til dato eller "så lenge hovedavtalen løper")

4. Kategorier personopplysninger

Følgende kategorier personopplysninger behandles:

- [ ] Identifikasjonsdata (navn, fødselsnummer, kontaktinformasjon)
- [ ] Ansettelses- og lønnsopplysninger
- [ ] Økonomiske opplysninger
- [ ] Helseopplysninger (særlig kategori, jf. art. 9)
- [ ] Opplysninger om straffedommer (art. 10)
- [ ] Tekniske data (IP-adresse, logger, enhetsinformasjon)
- [ ] Andre kategorier (spesifiser nedenfor)

Andre kategorier / presiseringer

5. Kategorier registrerte

- [ ] Ansatte hos behandlingsansvarlig
- [ ] Kunder / sluttbrukere
- [ ] Leverandører og samarbeidspartnere
- [ ] Pasienter / klienter
- [ ] Barn under 13 år
- [ ] Andre (spesifiser nedenfor)

Andre kategorier registrerte

6. Behandlingsansvarliges plikter

Behandlingsansvarlig har rettslig grunnlag for behandlingen etter GDPR art. 6 (og eventuelt art. 9/10), gir dokumenterte instrukser til databehandler og ivaretar de registrertes rettigheter. Behandlingsansvarlig kan til enhver tid endre eller utdype instruksene skriftlig.

7. Databehandlers plikter

Databehandler skal kun behandle personopplysninger etter dokumenterte instrukser fra behandlingsansvarlig, sørge for at personer med tilgang har taushetsplikt, bistå behandlingsansvarlig ved henvendelser fra registrerte, varsle om brudd uten ugrunnet opphold og stille nødvendig informasjon til rådighet for å dokumentere etterlevelse, jf. GDPR art. 28 nr. 3 bokstav a–h.

8. Sikkerhetstiltak (art. 32)

Databehandler skal gjennomføre egnede tekniske og organisatoriske tiltak for å sikre konfidensialitet, integritet, tilgjengelighet og robusthet. Følgende tiltak er minimum:

- [ ] Tilgangsstyring med personlig brukernavn og passord / SSO
- [ ] Kryptering av data under overføring (TLS 1.2+)
- [ ] Kryptering av data i hvile der det er relevant
- [ ] Logging av tilganger og endringer
- [ ] Regelmessig sikkerhetskopiering og testet gjenoppretting
- [ ] Opplæring av ansatte i personvern og informasjonssikkerhet
- [ ] ISO 27001, ISAE 3402 eller tilsvarende sertifisering

9. Bruk av underdatabehandlere

Databehandler kan benytte underdatabehandlere på følgende vilkår:

- [ ] Generell forhåndsgodkjenning – databehandler varsler minst 30 dager før endring
- [ ] Spesifikk godkjenning – hver underdatabehandler skal godkjennes skriftlig

Liste over godkjente underdatabehandlere ved avtaleinngåelse:

Godkjente underdatabehandlere (navn, land, formål)

10. Overføring til tredjeland

Overføring av personopplysninger til land utenfor EØS skal bygge på et gyldig overføringsgrunnlag etter

GDPR kapittel V, og databehandler skal gjennomføre en konkret risikovurdering (TIA) i tråd med Schrems II (C-311/18).

- [ ] Ingen overføring utenfor EØS
- [ ] Adekvansbeslutning fra EU-kommisjonen
- [ ] EUs standard personvernbestemmelser (SCC) av 2021
- [ ] EU-US Data Privacy Framework
- [ ] Bindende konsernregler (BCR)

11. Avviksvarsling

Databehandler skal uten ugrunnet opphold, og senest innen 24 timer etter at avviket er oppdaget, varsle behandlingsansvarlig skriftlig om brudd på personopplysningssikkerheten, jf. GDPR art. 33 nr. 2.

Varslingsadresse hos behandlingsansvarlig

---

12. Revisjon og tilsyn

Behandlingsansvarlig har rett til å gjennomføre revisjon, herunder inspeksjon, av databehandlers etterlevelse av avtalen. Databehandler kan dokumentere etterlevelse gjennom anerkjent tredjepartsrevisjon (f.eks. ISAE 3000/3402). Kostnader bæres av:

- [ ] Behandlingsansvarlig
- [ ] Databehandler ved påvist vesentlig brudd

13. Opphør og sletting

Ved avtalens opphør skal databehandler etter behandlingsansvarliges valg:

- [ ] Slette alle personopplysninger og bekrefte sletting skriftlig
- [ ] Tilbakelevere alle personopplysninger i avtalt format

Frist for sletting / tilbakelevering etter opphør

---

14. Ansvar og erstatning

Partene er ansvarlige etter GDPR art. 82 og personopplysningsloven § 30. Eventuell ansvarsbegrensning i hovedavtalen gjelder så langt den er forenlig med personvernregelverket.

Eventuell ansvarsbegrensning (beløp i NOK eller henvisning til hovedavtale)

---

15. Lovvalg og verneting

Avtalen reguleres av norsk rett. Tvister søkes løst ved forhandlinger. Verneting er:

Verneting (f.eks. Oslo tingrett)

---

16. Signatur

Avtalen er inngått elektronisk i to eksemplarer, ett til hver part. Signering med BankID via esigner.no gir tilsvarende rettsvirkning som håndskrevet signatur, jf. lov om elektroniske tillitstjenester.

Sted og dato	Behandlingsansvarlig (signatur)
Sted og dato	Databehandler (signatur)

Disse malene er et generelt utgangspunkt og er ikke juridisk rådgivning. Kontroller at innholdet passer din situasjon, og søk juridisk bistand ved tvil.

Last opp utfylt dokument på esigner.no og signer med BankID.