S103 – Databehandleravtale (DPA) – Envo AS

Versjon: 2
Gjelder fra: 01.03.2026
Utsteder: Envo AS

1. PARTER OG BAKGRUNN
Denne databehandleravtalen ("DPA") inngås mellom Kunden ("Behandlingsansvarlig") og Envo AS, org.nr. 998 082 625, Wirgenes vei 1, 3157 Barkåker ("Databehandler"). DPAen regulerer Databehandlers behandling av personopplysninger på vegne av Behandlingsansvarlig i forbindelse med levering av Envos programvarebaserte tjenester (SaaS) og tilhørende tjenester, jf. S105 – SaaS Tjenesteavtale ("SLA").

DPAen supplerer S102 – Alminnelige vilkår og S105 – SLA. Ved motstrid for personvernforhold skal denne DPAen ha forrang.

Denne DPAen anses akseptert og bindende når Kunden aksepterer Envos tilbud og/eller alminnelige vilkår, enten elektronisk eller ved faktisk bruk av Tjenestene

2. DEFINISJONER
Begreper som "personopplysninger", "behandling", "behandlingsansvarlig", "databehandler", "tilsynsmyndighet" og "brudd på personopplysningssikkerheten" skal ha den betydning som fremgår av GDPR. Øvrige udefinerte begreper har den betydning som følger av S102/S105.

3. GJENSTAND, VARIGHET OG FORMÅL
Databehandler behandler personopplysninger på vegne av Behandlingsansvarlig for å levere, drifte, vedlikeholde og videreutvikle Tjenestene, inkludert support, feilsøking, overvåking, sikkerhetstiltak og kundeadministrasjon. Detaljer fremgår av Vedlegg A (Behandlingsaktivitetene). Behandlingen pågår så lenge Behandlingsansvarlig benytter Tjenestene eller til sletting/retur etter § 12.

4. BEHANDLINGSGRUNNLAG OG DOKUMENTERTE INSTRUKSER
Databehandler skal kun behandle personopplysninger etter dokumenterte instrukser fra Behandlingsansvarlig. Instruksene kan være inntatt i denne DPAen, S102/S105, ordrebekreftelse/tilbud, samt skriftlig kommunikasjon mellom partene. Dersom en instruks er i strid med GDPR, skal Databehandler uten ugrunnet opphold varsle Behandlingsansvarlig.

5. KONFIDENSIALITET OG AUTORISASJON
Databehandler skal sikre at personer autorisert til å behandle personopplysninger har forpliktet seg til taushet eller er underlagt en passende lovpålagt taushetsplikt, og kun gis tilgang i den utstrekning som er nødvendig for formålet (need-to-know).

6. SIKKERHET – TEKNISKE OG ORGANISATORISKE TILTAK (TOMS)
Databehandler skal iverksette egnede tekniske og organisatoriske sikkerhetstiltak i henhold til GDPR artikkel 32. En oversikt over sentrale tiltak fremgår av Vedlegg C (Sikkerhetstiltak). Databehandler skal regelmessig vurdere effektiviteten av tiltakene, og kan oppdatere dem for å opprettholde et passende sikkerhetsnivå.

7. BRUDD PÅ PERSONOPPLYSNINGSSIKKERHETEN
Ved brudd på personopplysningssikkerheten skal Databehandler uten ugrunnet opphold varsle Behandlingsansvarlig. Varslet skal inneholde tilgjengelig informasjon i henhold til GDPR art. 33(3), og Databehandler skal løpende supplere informasjonen. Databehandler fører intern logg over hendelser.

8. BISTAND TIL BEHANDLINGSANSVARLIG
Hensyntatt behandlingens art og tilgjengelig informasjon skal Databehandler bistå Behandlingsansvarlig med: (i) oppfyllelse av registrertes rettigheter (kap. III), (ii) sikkerhet, varsling og avbøtende tiltak (art. 32–34), (iii) konsekvensvurderinger og forhåndsdrøftelser (art. 35–36), og (iv) oppfyllelse av forpliktelser etter art. 28. Rimelige, dokumenterte kostnader kan faktureres der bistanden går ut over det som følger av Tjenestene.

9. UNDERLEVERANDØRER (UNDERDATABEHANDLERE)
Behandlingsansvarlig gir Databehandler en generell fullmakt til å benytte underdatabehandlere spesifisert på Envos nettsider for leveransen. Oppdatert liste publiseres på Envos nettsider ("Subprocessor-listen"). Databehandler skal varsle Behandlingsansvarlig om tillegg/utskiftning med rimelig varsel via de

publiserte kanalene. Behandlingsansvarlig kan fremsette begrunnet innsigelse basert på personvernhensyn. Databehandler skal pålegge underdatabehandlerne tilsvarende forpliktelser som følger av denne DPAen og er ansvarlig for deres handlinger som for egne.

10. OVERFØRINGER UTENFOR EØS
Overføringer til tredjeland kan kun skje ved gyldig overføringsgrunnlag i henhold til GDPR kapittel V (tilstrekkelighetsbeslutning, EUs standard personvernbestemmelser (SCC), eller andre godkjente mekanismer). Der SCC benyttes, skal Databehandler og relevant mottaker inngå gjeldende modul(er). Databehandler skal informere Behandlingsansvarlig om relevante overføringsgrunnlag for behandlingen under Tjenestene.

11. REVISJON OG TILSYN
Databehandler skal gjøre tilgjengelig nødvendig informasjon for å påvise etterlevelse av denne DPAen og GDPR art. 28, og muliggjøre revisjon fra Behandlingsansvarlig eller en uavhengig revisor utpekt av Behandlingsansvarlig, etter rimelig varsel, innen normal arbeidstid og uten unødig forstyrrelser. Behandlingsansvarlig dekker egne kostnader; Databehandler dekker rimelige kostnader dersom revisjonen avdekker vesentlig brudd hos Databehandler.

12. SLETTING OG RETUR AV DATA
Ved opphør av Tjenestene eller etter skriftlig instruks fra Behandlingsansvarlig skal Databehandler, etter Behandlingsansvarligs valg, slette eller returnere personopplysninger og slette eksisterende kopier med mindre lagring kreves etter EØS-rett eller nasjonal rett. Databehandler tilbyr standard eksport i maskinlesbart format; tilpasset eksport kan leveres som tilleggstjeneste.

13. ANSVAR OG ERSTATNING
Partenes ansvar reguleres av S102 og gjeldende rett. Der GDPR fastsetter direkte erstatningsansvar overfor registrerte, gjelder dette i tillegg. Ingen bestemmelse i denne DPAen begrenser de rettigheter de registrerte har etter gjeldende rett.

14. LOVVALG, VERNETING OG VARIGHET
Denne DPAen er underlagt norsk rett. Verneting er Vestfold tingrett. DPAen gjelder så lenge Databehandler behandler personopplysninger på vegne av Behandlingsansvarlig i tilknytning til Tjenestene.

15. ENDRINGER
Databehandler kan oppdatere denne DPAen når det er nødvendig for å etterleve lov eller forbedre klarhet, med 60 dagers varsel gjennom publisering på Envos juridiske sider og/eller administrasjonsflate. Ved vesentlig endring som klart svekker Kundens rettigheter eller øker Kundens forpliktelser, kan Behandlingsansvarlig si opp berørte Tjenester med virkning fra ikrafttredelse ved skriftlig melding innen 14 dager etter varsel.

VEDLEGG A – BEHANDLINGSAKTIVITETENE
Formål: Leveranse, drift, vedlikehold og videreutvikling av Envos SaaS-tjenester (EMS/EPM m.fl.), inkludert feilretting, overvåking, sikkerhet og kundeadministrasjon.

Kategorier av registrerte: brukere hos Kunden (administratorer/sluttbrukere), Kundens ansatte/representanter, og andre personer som Kunden ber om at behandles i Tjenestene (f.eks. kontaktpersoner).

Kategorier av personopplysninger: identifikatorer (navn, e-post, telefon), brukerkonto-IDer, rolle/tilgang, logger og hendelser, tekniske metadata (IP, klientinfo), samt andre data som Kunden laster opp/konfigurerer. Envo behandler ikke særlige kategorier med mindre dette uttrykkelig er avtalt og dokumentert av Behandlingsansvarlig.

Behandlingsaktiviteter: innsamling etter instruks, registrering, strukturering, lagring, tilpasning, lesing/innsyn, bruk, overføring til autoriserte mottakere, begrensning, sletting og destruksjon.

Lagringssted: Primært innen EØS. Eventuelle tredjelands-overføringer skjer iht. § 10.

Varighet: Så lenge Avtalen løper eller til sletting/retur gjennomføres i henhold til § 12.

VEDLEGG B – UNDERDATABEHANDLERE
Underdatabehandlere som benyttes i dag:

Link Mobility AS benyttes for SMS-varslinger og meldingsformidling. Opplysninger som behandles er telefonnummer, meldingsinnhold og leveringsmetadata.

Copernica B.V. benyttes for utsendelse av e-post og kundekommunikasjon. Opplysninger som behandles er navn, e-postadresse, meldingsinnhold og metadata.

Ingen data fra våre underleverandører behandles utenfor EØS.

VEDLEGG C – TEKNISKE OG ORGANISATORISKE SIKKERHETSTILTAK
• Organisatorisk: ISMS/risikostyring, sikkerhetspolicy, opplæring og taushetserklæring, tilgangsstyring (prinsipp om minste privilegium), leverandørstyring og underleverandør-due diligence.

• Teknisk: nettverkssegmentering, brannmur/WAF, TLS i transitt, kryptering av data i ro hvor hensiktsmessig, multi-faktor autentisering, sikker programvareutvikling (SDLC), sårbarhetshåndtering og patching, overvåking og logging, sikkerhetskopi og gjenoppretting, høy tilgjengelighet i henhold til SLA.

• Prosess: hendelseshåndtering/beredskap, sikkerhetsrevisjoner/pen-testing, tilgangsresertifisering, endringskontroll, personvern-konsekvensvurderinger ved behov.