

Databehandleravtale

Klubben er behandlingsansvarlig for medlemmenes opplysninger, og EIT er databehandler. Denne avtalen inngås med hver klubb før EIT tas i bruk. Gule felt fylles ut før signering.

mellom **Klubbens navn**, org.nr. **org.nr.** (behandlingsansvarlig, heretter «Klubben»)

og **Leverandørens navn**, org.nr. **org.nr.**, som leverer tjenesten EIT (databehandler, heretter «Leverandøren»)

Avtalen er inngått i henhold til personvernforordningen (GDPR) artikkel 28 og personopplysningsloven. Den gjelder sammen med avtalen om bruk av EIT (hovedavtalen). Ved motstrid går denne avtalen foran når det gjelder behandling av personopplysninger.

1. Formål og omfang

1. Leverandøren behandler personopplysninger på vegne av Klubben for å levere EIT: medlemsregister, innsjekk og treningslogg, attest til våpensøknad, betaling, stevner, kurs, kalender og vakter, meldinger, klubbdrift (våpenutlån, nøkler, kasse, kontingent, dugnad, avvik, banesjekk, merkeskyting) og tilhørende funksjoner.
2. Klubben er behandlingsansvarlig og bestemmer formålet med behandlingen. Klubben er ansvarlig for at det finnes behandlingsgrunnlag, at medlemmene er informert (personvernerklæring), og for hvilke opplysninger klubbens administratorer legger inn.
3. Leverandøren skal bare behandle opplysningene slik denne avtalen og Klubbens dokumenterte instruksier. Bruk av funksjonene i EIT og innstillingene klubbens administratorer velger, regnes som Klubbens instruksier. Leverandøren skal si fra til Klubben hvis Leverandøren mener en instruks er i strid med regelverket.
4. Leverandøren skal ikke bruke opplysningene til egne formål, selge dem, bruke dem til markedsføring eller gi dem til andre, unntatt det som følger av punkt 6 eller av lov.

2. Hvilke opplysninger og hvem det gjelder

Registrerte

- Medlemmer og søkere om medlemskap
- Deltakere på kurs og stevner, også personer fra andre klubber
- Personer som får utlevert nøkler eller lånt klubbvåpen, og gjester ved merkeskyting
- Personer som er nevnt i avviksmeldinger og meldinger fra klubben

Kategorier av opplysninger

KATEGORI	EKSEMPLER
Identitet og kontakt	Navn, e-post, mobilnummer, fødselsdato, skytter-ID, profilbilde
Medlemskap	Rolle, kategori, status, forbund, kontingent og fritak
Aktivitet	Innsjekk (tid og bane), økter, resultater, stevner, kurs, godkjenninger, vakter, dugnadstimer
Betaling	Beløp, status og referanse fra Vipps. Kortnummer og bankopplysninger behandles ikke av EIT
Våpen og attest	Attester til våpensøknad, utlån av klubbvåpen (låntaker og fødselsdato), medlemmets egne våpen, serienummer og bilde av våpenkort
Dokumenter og bilder	Dokumenter medlemmet laster opp (kursbevis, startkort, medlemskort), bilder i skytedagboken, signaturer ved utlevering av nøkler
Kommunikasjon	Meldinger fra klubben, avviksmeldinger og oppfølging
Tekniske data	Innloggingsøkter, endringslogg for viktige handlinger, tekniske logger på serveren

EIT er ikke laget for særlige kategorier av personopplysninger (GDPR artikkel 9) eller opplysninger om straffbare forhold. Klubben skal begrense slike opplysninger. Avviksmeldinger om skader kan inneholde helseopplysninger – Klubben bør beskrive hendelsen uten å oppgi mer enn nødvendig.

3. Taushetsplikt og tilgang

1. Bare personer hos Leverandøren som trenger det for å drifte, feilsøke eller gi support, skal ha tilgang til opplysningene. De har taushetsplikt, også etter at de har sluttet.
2. Leverandøren ser ikke på Klubbens data uten at det trengs for drift, feilsøking eller support Klubben har bedt om. Tilgang til serveren logges.

4. Sikkerhet

1. Leverandøren skal gjennomføre egnede tekniske og organisatoriske tiltak etter GDPR artikkel 32. Tiltakene står i vedlegg A og kan forbedres uten at avtalen endres, men skal ikke svekkes.
2. Leverandøren skal regelmessig teste at tiltakene virker, blant annet at sikkerhetskopier kan gjenopprettes.

5. Brudd på personopplysningssikkerheten

1. Leverandøren skal varsle Klubben uten ugrunnet opphold, og senest 36 timer etter at bruddet ble oppdaget, slik at Klubben kan melde fra til Datatilsynet innen 72 timer.
2. Varselet skal så langt det er kjent beskrive hva som har skjedd, hvilke opplysninger og hvor mange registrerte som er berørt, sannsynlige konsekvenser og tiltak som er satt i verk. Informasjon som ikke er kjent ennå, ettersendes.
3. Leverandøren skal hjelpe Klubben med å melde bruddet og eventuelt informere de registrerte.

6. Underleverandører

1. Klubben godkjenner underleverandørene i vedlegg B. Leverandøren skal ha avtaler med dem som gir minst samme beskyttelse som denne avtalen.
2. Leverandøren skal varsle Klubben minst 30 dager før en ny underleverandør tas i bruk eller en underleverandør byttes ut. Klubben kan protestere med saklig grunn, og kan da si opp avtalen med virkning fra endringen.
3. Leverandøren er ansvarlig overfor Klubben for underleverandørenes behandling.

7. Overføring utenfor EU/EØS

Opplysningene lagres og behandles i Norge og EU/EØS. Leverandøren skal ikke overføre opplysninger til land utenfor EU/EØS uten skriftlig samtykke fra Klubben og et gyldig overføringsgrunnlag etter GDPR kapittel V.

8. Bistand til Klubben

1. EIT har funksjoner for innsyn, retting, sletting og dataportabilitet: medlemmet ser og retter egne opplysninger og laster ned egen treningslogg, administrator kan rette og slette medlemmer, og alle Klubbens data kan eksporteres. Trenger Klubben mer hjelp til å oppfylle de registrertes rettigheter, skal Leverandøren bistå.
2. Leverandøren skal hjelpe Klubben med vurderinger av personvernkonsekvenser og forhåndsdrøftinger med Datatilsynet når det er relevant.
3. Henvendelser fra registrerte som kommer til Leverandøren, sendes videre til Klubben uten å besvares, med mindre Klubben har bedt om noe annet.

9. Revisjon og dokumentasjon

1. Leverandøren skal gi Klubben den informasjonen som trengs for å vise at avtalen følges.
2. Klubben kan én gang i året, eller etter et sikkerhetsbrudd, be om en gjennomgang av sikkerhetstiltakene. Gjennomgangen avtales med rimelig varsel og gjøres så langt mulig skriftlig. Hver part dekker egne kostnader.

10. Varighet, oppsigelse og sletting

1. Avtalen gjelder så lenge Leverandøren behandler personopplysninger for Klubben.

2. Klubbens administrator kan når som helst laste ned alle Klubbens data (CSV og JSON) under Klubbinnstillinger → Eksport av alle data.
3. Når hovedavtalen opphører, sletter Leverandøren Klubbens data innen 30 dager, med mindre Klubben skriftlig ber om en annen frist eller lov krever lagring. Sikkerhetskopier slettes når de roterer ut, senest 35 dager etter slettingen. Leverandøren bekrefter slettingen skriftlig på forespørsel.
4. Brukerkontoer som også er medlem i andre klubber i EIT, beholdes, men alle opplysninger knyttet til Klubben slettes.

11. Ansvar

Partenes ansvar følger GDPR artikkel 82. For øvrig gjelder ansvarsbegrensningene i hovedavtalen, så langt de ikke strider mot regelverket.

12. Lovvalg og tvister

Avtalen reguleres av norsk rett. Tvister skal først søkes løst ved forhandlinger. Hvis det ikke lykkes, er **verneting, f.eks. Leverandørens hjemting** avtalt verneting.

13. Kontaktpersoner

	KLUBBEN	LEVERANDØREN
Navn	navn	navn
E-post	e-post	post@eit.no
Telefon	telefon	telefon

Endringer i kontaktpersoner meldes skriftlig.

Underskrifter

Avtalen er inngått i to eksemplarer, ett til hver part, eller signert elektronisk.

Sted og dato

For Klubben: **navn og rolle**

Sted og dato

For Leverandøren: **navn og rolle**

Vedlegg A – Sikkerhetstiltak

OMRÅDE	TILTAK
Plassering	Server hos hostingleverandør i land i EU/EØS . Ingen lagring utenfor EU/EØS
Overføring	All trafikk kryptert med HTTPS (TLS 1.2 eller nyere) og HSTS
Lagring	Dokumenter, våpenkort, bilder, signaturer og klubbenes Vipps- og SMS-nøkler krypteres med AES-256-GCM. Nøkkelen lagres atskilt fra databasen
Passord	Lagres som bcrypt-hash. Innlogging med Vipps er mulig. Gjentatte feilforsøk stoppes
Tilgang i appen	Roller (medlem, skyteleder, administrator). Klubber er skilt fra hverandre. Ingen kan godkjenne egne økter eller attester
Applikasjonssikkerhet	Beskyttelse mot CSRF, sikkerhetshoder (CSP), begrensning av forespørsler, kontroll av filtype på opplastinger
Tilgang til serveren	Bare navngitte personer hos Leverandøren, med SSH-nøkler og tofaktorautentisering. Tilgang logges
Sikkerhetskopier	Hver natt. Lagres på serveren, på et annet sted i Norge og i skylagring i EU/EØS. De 30 siste beholdes. Gjenoppretting testes hvor ofte, f.eks. hvert kvartal
Oppdateringer	Sikkerhetsoppdateringer av operativsystem, Docker og avhengigheter legges inn fortløpende
Logging	Endringslogg for viktige handlinger i appen. Tekniske logger på serveren slettes etter antall dager
Overvåking	Tjenesten overvåkes, og Leverandøren varsles ved nedetid

Vedlegg B – Underleverandører

UNDERLEVERANDØR	HVA	PLASSERING
navn	Drift av server, database og filer	land i EU/EØS
navn	Skylagring av sikkerhetskopier	land i EU/EØS
navn eller «Leverandøren selv»	Sikkerhetskopier på et annet sted i Norge	Norge
navn	Utsending av e-post (passord, varsler, meldinger)	land i EU/EØS
navn, f.eks. Sveve AS	Utsending av SMS – bare når Klubben bruker EITs felles SMS-oppsett	land

Ikke underleverandører under denne avtalen:

- **Vipps MobilePay:** Klubben har sin egen avtale med Vipps MobilePay for betaling. For «Logg inn med Vipps» er Vipps MobilePay selvstendig behandlingsansvarlig for innloggingen.
- **Klubbens egen SMS-leverandør:** Bruker Klubben sin egen SMS-avtale, er den leverandøren Klubbens egen databehandler.
- **Push-varsler:** Varsler til mobilen sendes via nettleserens push-tjeneste (f.eks. Google, Apple, Mozilla). Innholdet er ende-til-ende-kryptert, så tjenesten kan ikke lese det.
- **MET Norge:** Værvarselet på storskjermen hentes uten personopplysninger.

Versjon 1.0 · oktober 2026