

Databehandleravtale for Fastlegeweb

Etter personvernforordningen (GDPR) artikkel 28 · Versjon 1.0 · 11. september 2026

Parter

	Behandlingsansvarlig (Kunden)	Databehandler (Leverandøren)
Navn		TK DIGITAL AS
Org.nr.		932 383 284 MVA
Adresse		Nedre Åsenvei 6C, 3215 Sandefjord
Kontaktperson for personvern		Håkon Kiær
E-post		hei@fastlegeweb.no

Kunden omtales nedenfor som «den behandlingsansvarlige», og TK DIGITAL AS som «Databehandleren».

1. Bakgrunn og formål

1.1 Partene har inngått lisensavtale om Fastlegeweb («Hovedavtalen»). Når Databehandleren leverer Fastlegeweb («Løsningen»), behandler Databehandleren personopplysninger på vegne av den behandlingsansvarlige.

1.2 Denne avtalen skal sikre at behandlingen skjer i samsvar med personopplysningsloven og personvernforordningen (forordning (EU) 2016/679, «GDPR»), særlig artikkel 28.

1.3 Avtalen bygger på EU-kommisjonens standard personvernbestemmelser for avtaler mellom behandlingsansvarlige og databehandlere (gjennomføringsbeslutning (EU) 2021/915), tilpasset Løsningen.

1.4 Ved motstrid mellom denne avtalen og Hovedavtalen gjelder denne avtalen foran i spørsmål om behandling av personopplysninger.

2. Definisjoner

Begrepene i denne avtalen, som «personopplysninger», «behandling», «behandlingsansvarlig», «databehandler», «registrert» og «brudd på personopplysningssikkerheten», har samme betydning som i GDPR artikkel 4.

3. Behandlingens formål og omfang

3.1 Formålet med behandlingen, hvilke personopplysninger som behandles og hvem de gjelder, er beskrevet i vedlegg A.

3.2 Databehandleren skal ikke behandle personopplysningene for egne formål.

4. Instrukser

4.1 Databehandleren skal bare behandle personopplysninger etter dokumenterte instrukser fra den behandlingsansvarlige. Hovedavtalen, denne avtalen og den behandlingsansvarliges egen bruk av administrasjonspanelet i Løsningen (å legge inn, endre og slette innhold) utgjør instruksene. Andre instrukser skal gis skriftlig.

4.2 Databehandleren skal straks varsle den behandlingsansvarlige dersom en instruks etter Databehandlerens vurdering er i strid med personvernregelverket.

4.3 Er Databehandleren pålagt ved lov å behandle personopplysninger på annen måte, skal den behandlingsansvarlige varsles om dette før behandlingen starter, med mindre loven forbyr slik varsling.

5. Den behandlingsansvarliges plikter

5.1 Den behandlingsansvarlige er ansvarlig for at behandlingen har et lovlig grunnlag, og for at de registrerte får informasjon om behandlingen. Dette gjelder blant annet opplysninger og bilder av ansatte som publiseres på nettsiden.

5.2 Den behandlingsansvarlige skal ikke legge inn helseopplysninger, opplysninger om pasienter eller andre særlige kategorier av personopplysninger (GDPR artikkel 9 og 10) i Løsningen.

6. Taushetsplikt

6.1 Databehandleren skal sørge for at alle som har tilgang til personopplysningene, har taushetsplikt. Tilgang gis bare til dem som trenger det for å levere Løsningen.

6.2 Taushetsplikten gjelder også etter at avtalen er opphørt.

7. Informasjonssikkerhet

7.1 Databehandleren skal gjennomføre egnede tekniske og organisatoriske tiltak for å sikre et sikkerhetsnivå som passer til risikoen, jf. GDPR artikkel 32. Tiltakene er beskrevet i vedlegg C.

7.2 Databehandleren skal løpende vurdere risikoen og oppdatere tiltakene ved behov. Endringer skal ikke redusere det samlede sikkerhetsnivået.

8. Bistand til den behandlingsansvarlige

8.1 Databehandleren skal bistå den behandlingsansvarlige med å oppfylle de registrertes rettigheter etter GDPR kapittel III, som retten til innsyn, retting og sletting. Henvendelser fra registrerte skal videresendes til den behandlingsansvarlige uten ugrunnet opphold. Databehandleren skal ikke selv svare på henvendelsen, med mindre den behandlingsansvarlige har gitt beskjed om det.

8.2 Databehandleren skal også bistå den behandlingsansvarlige med å oppfylle pliktene etter GDPR artikkel 32 til 36, om sikkerhet, melding av avvik, vurdering av personvernkonsekvenser og forhåndsdrøftinger med Datatilsynet. Bistanden gis ut fra behandlingens art og den informasjonen Databehandleren har tilgjengelig.

9. Brudd på personopplysningssikkerheten

9.1 Databehandleren skal varsle den behandlingsansvarlige uten ugrunnet opphold, og senest 48 timer etter at Databehandleren ble kjent med et brudd på personopplysningssikkerheten. Dette gir den behandlingsansvarlige mulighet til å melde avviket til Datatilsynet innen fristen på 72 timer i GDPR artikkel 33.

9.2 Varselet skal så langt det er mulig inneholde:

- en beskrivelse av bruddet, herunder hvilke kategorier og omtrent hvor mange registrerte og personopplysninger som er berørt
- sannsynlige konsekvenser av bruddet
- tiltak som er gjennomført eller foreslått for å håndtere bruddet og begrense skadevirkningene
- kontaktpunkt hos Databehandleren

9.3 Er det ikke mulig å gi all informasjon samtidig, kan den gis trinnvis uten ugrunnet opphold. Databehandleren skal dokumentere alle brudd på personopplysningssikkerheten.

10. Underdatabehandlere

10.1 Den behandlingsansvarlige gir generell forhåndsgodkjenning til at Databehandleren bruker underdatabehandlere. Underdatabehandlerne som brukes når avtalen inngås, er listet i vedlegg B.

10.2 Databehandleren skal varsle den behandlingsansvarlige skriftlig minst 30 dager før en ny underdatabehandler tas i bruk eller en eksisterende byttes ut. Den behandlingsansvarlige kan protestere mot endringen på saklig grunnlag. Blir partene ikke enige, kan den behandlingsansvarlige si opp Hovedavtalen og denne avtalen med virkning før endringen trer i kraft, og får da refundert forhåndsbetalt vederlag for gjenværende periode forholdsmessig.

10.3 Databehandleren skal inngå skriftlig avtale med underdatabehandlere som pålegger dem minst de samme pliktene som følger av denne avtalen. Databehandleren er fullt ansvarlig overfor den behandlingsansvarlige for underdatabehandlernes oppfyllelse av sine plikter.

11. Overføring til land utenfor EØS

11.1 Personopplysningene lagres og behandles i EØS.

11.2 Overføring av personopplysninger til land utenfor EØS kan bare skje med gyldig overføringsgrunnlag etter GDPR kapittel V, som en beslutning om tilstrekkelig beskyttelsesnivå eller EUs standard personvernbestemmelser. Nye overføringer skal varsles som angitt i punkt 10.2.

12. Dokumentasjon og revisjon

12.1 Databehandleren skal gjøre tilgjengelig all informasjon som er nødvendig for å vise at pliktene i denne avtalen og GDPR artikkel 28 er oppfylt.

12.2 Den behandlingsansvarlige, eller en uavhengig revisor den behandlingsansvarlige utpeker, kan gjennomføre revisjon av Databehandleren. Revisjon varsles minst 30 dager i forveien, gjennomføres i ordinær arbeidstid og kan skje én gang per år, med mindre et brudd på personopplysningssikkerheten eller pålegg fra Datatilsynet gir grunn til hyppigere revisjon. Den behandlingsansvarlige dekker egne kostnader ved revisjonen.

12.3 For underdatabehandlere kan revisjonsplikten oppfylles ved å vise til deres uavhengige sertifiseringer og revisjonsrapporter, som ISO 27001 og SOC 2.

13. Varighet og opphør

13.1 Avtalen gjelder så lenge Databehandleren behandler personopplysninger på vegne av den behandlingsansvarlige.

13.2 Når Hovedavtalen opphører, kan den behandlingsansvarlige innen 30 dager kreve sitt innhold utlevert, jf. Hovedavtalen punkt 8. Databehandleren skal slette alle personopplysninger som behandles på vegne av den behandlingsansvarlige, senest 30 dager etter at Hovedavtalen er opphørt, eller etter at innholdet er utlevert dersom det skjer senere.

13.3 Sikkerhetskopier overskrives fortløpende, og personopplysningene er slettet også fra disse senest 30 dager etter slettingen i punkt 13.2.

13.4 Databehandleren skal på forespørsel bekrefte skriftlig at slettingen er gjennomført.

14. Ansvar

Hver av partene er ansvarlig etter GDPR artikkel 82. Ansvarsbegrensningene i Hovedavtalen gjelder også for denne avtalen, så langt ikke annet følger av ufravikelig lov.

15. Lovvalg og tvister

Avtalen reguleres av norsk rett. Tvister avgjøres av de alminnelige domstoler, med Oslo tingrett som avtalt vernetting.

Signaturer

For den behandlingsansvarlige (Kunden)	For Databehandleren (TK DIGITAL AS)
Sted og dato	Sted og dato
Navn og stilling	Navn og stilling
Signatur	Signatur

Vedlegg A – Beskrivelse av behandlingen

Formål. Levere Løsningen til den behandlingsansvarlige: drift og hosting av legekontorets nettside og administrasjonspanel, sikkerhetskopiering, feilsøking og kundestøtte.

Behandlingens art. Lagring, strukturering, publisering på nettsiden, sikkerhetskopiering, teknisk logging og sletting.

Registrerte og personopplysninger.

Registrerte	Personopplysninger	Kilde
Ansatte ved legekontoret som presenteres på nettsiden	Navn, stillingstittel, beskrivelse og bilde	Legges inn av den behandlingsansvarlige
Brukere av administrasjonspanelet	Navn, brukernavn, e-postadresse, passord (lagret kun som kryptografisk hash) og tidspunkt for innlogging	Den behandlingsansvarlige
Personer som omtales i fritekst, for eksempel i nyheter og varsler	Opplysningene den behandlingsansvarlige selv velger å skrive inn	Legges inn av den behandlingsansvarlige
Besøkende på nettsiden	IP-adresse, nettlesertype, tidspunkt og hvilken side som ble besøkt (serverlogg). Nødvendige informasjonskapsler for sikkerhet og innlogging	Registreres automatisk

Særlige kategorier av personopplysninger. Ingen. Løsningen er ikke laget for helseopplysninger eller andre særlige kategorier, jf. punkt 5.2.

Varighet. Så lenge Hovedavtalen gjelder, og deretter til sletting etter punkt 13. Serverlogger slettes automatisk etter 30 dager. Sikkerhetskopier av databasen overskrives fortløpende og bevares i omtrent 20 dager.

Behandlingssted. Google Cloud, region europe-north1 (Finland).

Vedlegg B – Underdatabehandlere

Underdatabehandler	Tjeneste	Behandlingssted
Google Cloud EMEA Limited, Dublin, Irland (Google Cloud)	Drift av nettsiden (Cloud Run), database (Cloud SQL), lagring av bilder (Cloud Storage), lagring av nøkler (Secret Manager) og serverlogger (Cloud Logging)	EØS: region europe-north1 (Finland)
Google Cloud EMEA Limited, Dublin, Irland (Google Workspace)	E-post med automatiske feilvarsler til Databehandleren. Varslene kan inneholde tekniske opplysninger om forespørselen som feilet, som IP-adresse, nettadresse og brukernavn.	EØS og andre land

Google behandler personopplysningene etter Googles databehandlervilkår (Cloud Data Processing Addendum). Eventuell tilgang fra land utenfor EØS, for eksempel ved teknisk support, har overføringsgrunnlag i EU–US Data Privacy Framework og EUs standard personvernbestemmelser.

Eksterne ressurser på nettsiden. Nettsiden henter skrifttyper og ikonbiblioteker fra Google Fonts, jsDelivr og cdnjs (Cloudflare). Den besøkendes nettleser laster ned disse filene direkte fra tilbyderne, som dermed mottar den besøkendes IP-adresse. Tilbyderne mottar ingen opplysninger fra Løsningens database.

Vedlegg C – Sikkerhetstiltak

Tilgangskontroll

- Hvert legekontor har egne brukerkontoer, og tilgangen i administrasjonspanelet er begrenset til legekontorets egne data.
- Passord lagres bare som kryptografisk hash, aldri i klartekst.
- Tilgang til driftsmiljøet er begrenset til Databehandlerens utviklere, med personlige kontoer beskyttet med totrinnsverifisering.
- Løsningen kjører med en tjenestekonto som bare har de rettighetene den trenger.

Kryptering

- All trafikk til og fra nettsiden krypteres med HTTPS (TLS), og informasjonskapsler for innlogging sendes bare over kryptert forbindelse.
- Database, lagrede filer og sikkerhetskopier er kryptert ved lagring.
- Nøkler og passord til tjenester lagres i Google Secret Manager, ikke i kildekoden.

Tilgjengelighet og gjenoppretting

- Databasen sikkerhetskopieres automatisk hver dag.
- Løsningen driftes i Google Clouds datasenter i Finland, som har fysisk sikring, redundant strøm og nettverk, og uavhengige sertifiseringer som ISO 27001 og SOC 2.

Drift og vedlikehold

- Programvare og avhengigheter holdes oppdatert med sikkerhetsoppdateringer.
- Automatiserte tester kjøres før nye versjoner settes i produksjon.
- Feil i produksjon varsles automatisk til Databehandleren.

Dataminimering

- Løsningen bruker ikke analyseverktøy eller sporings-cookies på legekontorets nettside, og samler ikke inn opplysninger om besøkende utover tekniske serverlogger.
- Serverlogger slettes automatisk etter 30 dager.

Organisatoriske tiltak

- Alle med tilgang til personopplysninger har taushetsplikt.
- Brudd på personopplysningssikkerheten håndteres og varsles som beskrevet i punkt 9.