

Databehandleravtale

Avtale om behandling av personopplysninger mellom skoleeier (behandlingsansvarlig) og NiceLab AS (databehandler) for Mattetime.

Versjon	1.0
Status	Gjeldende versjon
Oppdatert	8. september 2026
Databehandler	NiceLab AS, org.nr. 936 966 497, hjelp@mattetime.no
Gjeldende versjon	https://mattetime.no/personvern/databehandleravtale

Innhold

Databehandleravtale	3
1. Parter og bakgrunn	3
2. Formål, art og varighet	3
3. Kategorier av registrerte og opplysninger	3
4. Leverandørens plikter	3
5. Kundens plikter	4
6. Hvor opplysningene behandles og lagres	5
7. Sletting og lagringstid	5
8. Revisjon og dokumentasjon	5
9. Ansvar og erstatning	5
10. Varighet og opphør	5
11. Endringer i avtalen	6
12. Lovvalg og verneting	6
13. Kontaktpunkter	6
14. Signatur	6
Vedlegg A: Behandlinger, datakategorier og lagringstid	7
Dataminimering som er bygget inn	7
Sletting	7
Vedlegg B: Tekniske og organisatoriske sikkerhetstiltak	9
Identitet og tilgang	9
Data	9
Transport, lagring og drift	9
Logging	10
Hendelseshåndtering	10
Universell utforming	10
Vedlegg C: Underdatabehandlere og lokasjon	11
Egen drift	11
Ikke i bruk	11
Versjonshistorikk	12

Databehandleravtale

1. Parter og bakgrunn

- **Behandlingsansvarlig:** Skoleeier (kommune, fylkeskommune eller privat skoleeier), heretter «Kunden».
- **Databehandler:** NiceLab AS, org.nr. 936 966 497, heretter «Leverandøren».

Avtalen regulerer Leverandørens behandling av personopplysninger på vegne av Kunden i tjenesten Mattetime, i samsvar med personvernforordningen (EU) 2016/679 («GDPR») artikkel 28 og personopplysningsloven. Begreper brukes slik de er definert i GDPR artikkel 4.

Avtalen er et vedlegg til hovedavtalen om Mattetime og gjelder for alle skoler og enheter Kunden har lagt inn i tjenesten. Ved motstrid om behandling av personopplysninger går denne avtalen foran hovedavtalen.

2. Formål, art og varighet

Leverandøren behandler personopplysninger for å levere Mattetime: matematikkøving for elever, administrasjon av klasser og brukere, og resultater til læreren. Behandlingen består i innsamling, lagring, strukturering, visning for autoriserte brukere, sikkerhetskopiering og sletting. Behandlingene, kategoriene og standard lagringstid er beskrevet i Vedlegg A. Behandlingen varer så lenge hovedavtalen gjelder, med tillegg av slettefristen i punkt 4.9.

3. Kategorier av registrerte og opplysninger

Registrerte	Opplysninger
Elever	Fornavn eller visningsnavn, klasse, trinn, kortkode (hash), svar og resultater i aktiviteter, tilpasninger (ekstra tid, hint)
Lærere og administratorer	Navn, e-post, rolle, passordhash, tofaktorhemmelighet (kryptert), innloggingshistorikk
Gjester uten konto	Selvvalgt alias i én aktivitet; anonymiseres 24 timer etter avsluttet aktivitet

Ingen særlige kategorier av personopplysninger (GDPR artikkel 9). Ingen fødselsnummer, fødselsdato eller e-post for elever.

4. Leverandørens plikter

1. **Instruks.** Behandler bare etter dokumentert instruks fra Kunden: denne avtalen, hovedavtalen og innstillingene Kunden gjør i tjenesten. Dette gjelder også overføring til land utenfor EU/EØS, som ikke skjer, se punkt 6.
2. **Varsel om ulovlig instruks.** Varsler Kunden umiddelbart dersom Leverandøren mener en instruks er i strid med GDPR eller annen personvernlovgivning, og kan avvente behandlingen til instruksjonen er avklart.
3. **Konfidensialitet.** Sikrer at bare personer som trenger tilgang for å levere tjenesten får det, at de er underlagt taushetsplikt som varer etter at oppdraget er avsluttet, og at all tilgang til kundedata logges i revisjonsloggen. Leverandøren logger seg aldri inn som en annen bruker.

4. **Sikkerhet.** Iverksetter de tekniske og organisatoriske tiltakene som er beskrevet i Vedlegg B (GDPR artikkel 32), og opprettholder minst dette nivået gjennom avtaletiden.
5. **Underdatabehandlere.** Bruker bare underdatabehandlere som står i Vedlegg C. Kunden gir ved signering en generell godkjenning av disse. Leverandøren varsler Kunden minst 30 dager før en ny underdatabehandler tas i bruk eller en eksisterende byttes ut. Kunden kan motsette seg endringen innen fristen; partene skal da søke en løsning, og Kunden kan si opp avtalen med virkning fra endringen dersom en løsning ikke finnes. Leverandøren pålegger underdatabehandlere de samme forpliktelsene som følger av denne avtalen gjennom skriftlig avtale, og er fullt ansvarlig overfor Kunden for underdatabehandlernes oppfyllelse.
6. **Bistand med de registrertes rettigheter.** Bistår Kunden med innsyn, retting, sletting, begrensning, dataportabilitet og innsigelser (GDPR artikkel 15–22). Det meste er selvbetjent i tjenesten; øvrige henvendelser besvares innen 10 virkedager. Henvendelser fra registrerte som kommer direkte til Leverandøren, videresendes til Kunden uten ugrunnet opphold og besvares ikke av Leverandøren på egen hånd.
7. **Bistand med sikkerhet, DPIA og forhåndsdrøfting.** Bistår Kunden med å oppfylle GDPR artikkel 32–36, herunder personvernkonsekvensvurdering (DPIA) og eventuell forhåndsdrøfting med Datatilsynet, ved å levere faktagrunnlag om behandlingen på forespørsel.
8. **Brudd på personopplysningssikkerheten.** Varsler Kunden uten ugrunnet opphold og senest 48 timer etter at Leverandøren har oppdaget et brudd. Varselet skal så langt det er kjent beskrive bruddets art, hvilke kategorier og omtrent hvor mange registrerte og opplysninger som er berørt, sannsynlige konsekvenser, iverksatte og foreslåtte tiltak, og et kontaktpunkt. Opplysninger som ikke er kjent ved første varsel, ettersendes uten ugrunnet opphold. Leverandøren varsler ikke Datatilsynet eller de registrerte på egen hånd, men bistår Kunden med dette.
9. **Sletting og retur ved opphør.** Sletter eller returnerer alle personopplysninger ved avtalens opphør etter Kundens valg, senest 90 dager etter, og sletter eksisterende kopier, med mindre lov krever lengre lagring. Sikkerhetskopier slettes etter hvert som de roterer ut, senest 30 dager etter hovedslettingen. Kunden kan når som helst eksportere egne data fra tjenesten.
10. **Dokumentasjon og revisjon.** Gjør tilgjengelig all informasjon som er nødvendig for å påvise at pliktene i denne avtalen og GDPR artikkel 28 er oppfylt, se punkt 8.
11. **Protokoll.** Fører protokoll over behandlingskategorier på vegne av Kunden (GDPR artikkel 30 nr. 2) og gjør den tilgjengelig for Kunden på forespørsel.

5. Kundens plikter

- Er behandlingsansvarlig og har rettslig grunnlag for behandlingen (normalt opplæringsloven og offentlig myndighetsutøvelse).
- Gir Leverandøren dokumenterte instruksjoner gjennom avtalen og innstillingene i tjenesten, og sørger for at instruksene er lovlige.
- Sørger for at brukerne ikke registrerer mer enn nødvendig: bare fornavn på elever, ingen fritekst om barn.
- Administrerer roller og tilganger i egen organisasjon, og fjerner brukere som ikke lenger skal ha tilgang.
- Vurderer selv om behandlingen krever DPIA, og gjennomfører den med Leverandørens underlag.
- Informerer de registrerte (elever, foresatte, ansatte) om behandlingen i samsvar med GDPR artikkel 13 og 14.

6. Hvor opplysningene behandles og lagres

All behandling og lagring skjer i datasenteret til Hetzner Online GmbH i **Helsinki, Finland**. Det gjelder applikasjonsserverne, databasen, mellomlageret og de krypterte sikkerhetskopiene.

- Ingen kundedata behandles eller lagres i andre Hetzner-datasentre (for eksempel i Tyskland).
- Ingen overføring til land utenfor EU/EØS. Skulle en overføring bli nødvendig, krever den Kundens dokumenterte instruks på forhånd og et gyldig overføringsgrunnlag etter GDPR kapittel V.
- Cloudflare terminerer kryptert trafikk foran tjenesten og lagrer ikke innhold. E-post til voksne brukere sendes via Resend i EU-regionen. Se Vedlegg C.

Dersom Leverandøren planlegger å flytte behandlingen til et annet datasenter innenfor EU/EØS, varsles Kunden som ved endring av underdatabehandler (punkt 4.5).

7. Sletting og lagringstid

Standard lagringstid er satt for å dekke et skoleår med oppfølging, og kan avtales annerledes per kunde i hovedavtalen:

Data	Standard
Gjester uten konto	Anonymiseres 24 timer etter avsluttet aktivitet
Elevsvar (rådata)	365 dager etter avsluttet aktivitet
Slettede brukere	30 dagers karantene, deretter fjernes personidentifikatorer fysisk
Revisjonslogg	730 dager

Sletting kjøres som dokumenterte jobber med resultat, slik at Kunden kan få bekreftet at sletting er gjennomført. Kunden kan be om sletting av enkeltopplysninger eller hele skoler tidligere enn standardfristene.

8. Revisjon og dokumentasjon

Kunden kan én gang per år be om skriftlig dokumentasjon på at Leverandøren etterlever avtalen, og kan etter nærmere avtale med minst 14 dagers varsel gjennomføre revisjon selv eller ved en uavhengig tredjepart underlagt taushetsplikt. Revisjonen skal gjennomføres i ordinær arbeidstid og slik at den ikke forstyrrer andre kunders drift eller avslører deres data. Leverandøren dekker egne kostnader ved én revisjon per år; ytterligere revisjoner dekkes av Kunden med mindre revisjonen avdekker vesentlige avvik. Leverandøren bistår også ved tilsyn fra Datatilsynet.

9. Ansvar og erstatning

Partenes ansvar overfor hverandre for brudd på denne avtalen følger hovedavtalens bestemmelser om ansvar og erstatning. Ansvar overfor registrerte og tilsynsmyndighet følger GDPR artikkel 82 og 83. Leverandøren er ansvarlig for underdatabehandlere som for egne handlinger.

10. Varighet og opphør

Avtalen gjelder så lenge hovedavtalen gjelder og kan ikke sies opp separat mens Leverandøren behandler personopplysninger for Kunden. Ved opphør gjelder punkt 4.9 om sletting og retur. Punktene om konfidensialitet og ansvar gjelder også etter opphør.

11. Endringer i avtalen

Avtalen er versjonert. Gjeldende versjon er alltid tilgjengelig på mattetime.no/personvern/ databehandleravtale med versjonshistorikk. Endringer som svekker Kundens rettigheter, utvider behandlingen eller berører punkt 4, 6 eller 7, varsles med minst 30 dagers frist og krever Kundens aksept. Endringer som følger av ny lovgivning eller pålegg fra tilsynsmyndighet, og rettelser som ikke endrer innholdet, varsles uten frist. Ved uenighet gjelder sist aksepterte versjon til partene er enige eller avtalen opphører.

12. Lovvalg og verneting

Avtalen er underlagt norsk rett. Tvister løses ved forhandlinger. Fører ikke det fram, kan hver av partene bringe saken inn for Kundens alminnelige verneting.

13. Kontaktpunkter

- **Leverandøren:** hjelp@mattetime.no (merk henvendelsen «Personvern»). Bruddvarsel sendes til Kundens oppgitte kontaktpunkt og til den e-postadressen Kundens administrator er registrert med i tjenesten.
- **Kunden:** oppgir kontaktpunkt for personvern (for eksempel personvernombud) ved signering og holder det oppdatert i tjenesten.

14. Signatur

Avtalen signeres digitalt av person med signaturrett hos hver part. Versjonsnummer og signeringsdato registreres på Kundens avtale hos Leverandøren.

For Kunden (behandlingsansvarlig)	For NiceLab AS (databehandler)
Navn:	Navn:
Stilling:	Stilling:
Kontaktpunkt for personvern:	hjelp@mattetime.no
Sted og dato:	Sted og dato:
Signatur:	Signatur:

Vedlegg A: Behandlinger, datakategorier og lagringstid

Vedlegget beskriver hvilke opplysninger Leverandøren behandler for Kunden, hvorfor, og hvor lenge de beholdes som standard.

Kategori	Eksempler	Registrert	Formål	Lagringstid (standard)
Kundeadministrasjon	Organisasjonsnavn, org.nr., fakturaadresse, kontaktperson	Skoleeier	Avtale og fakturering	Avtaletid + 5 år (bokføringsloven)
Voksne brukere	Navn, e-post, passordhash, kryptert tofaktorhemmelighet, roller, innlogginger	Lærer, administrator	Innlogging og tilgangsstyring	Til brukeren slettes + 30 dagers karantene
Elevprofil	Fornavn, trinn, klasse, kortkode-hash, tilpasninger	Elev	Deltakelse og lærerens oppfølging	Skoleår + 12 måneder, konfigurerbart
Læringsdata	Svar, forsøk, tid og resultat per oppgave	Elev	Tilbakemelding til eleven og oppfølging fra læreren	Rådata 365 dager etter avsluttet aktivitet
Gjestedeltakelse	Selvvalgt alias, svar i én aktivitet	Gjest	Demonstrasjon uten konto	Anonymiseres 24 timer etter avsluttet aktivitet
Eksterne identiteter	Feide-id eller Google-id, hvis Kunden bruker det	Lærer, administrator, elev	Innlogging	Som brukeren
Revisjonslogg	Aktør, handling, mål, IP-adresse, tidspunkt	Lærer, administrator, Leverandørens ansatte	Sikkerhet og etterprøvbarehet	730 dager
Tekniske logger	Request-id, feil, ytelse	Alle	Drift og feilsøking	30 dager

Dataminimering som er bygget inn

- Elever registreres med fornavn. Import avviser e-post og tall.
- Ingen fødselsdato: trinn brukes i stedet for alder.
- Kortkoder lagres som hash med skolens id som salt, og kan trekkes tilbake.
- Fritekst fra elever begrenses til et alias ved gjestedeltakelse (maks 30 tegn).
- Overordnede nivåer (organisasjon, enhet) ser aggregater per skole, ikke enkeltbarns svar.
- Ingen automatisert profilering, ingen diagnose og ingen adaptiv vurdering av barnet.
- De åpne spillene uten innlogging lagrer ingenting hos Leverandøren; fremgang ligger i nettleseren.

Sletting

Sletting kjøres som dokumenterte jobber med resultat. Myk sletting brukes i karanteneperioden slik at

feil kan rettes, deretter fjernes personidentifikatorer fysisk fra databasen og fra sikkerhetskopier etter hvert som de roterer ut.

Vedlegg B: Tekniske og organisatoriske sikkerhetstiltak

Tiltakene under er bygget inn i tjenesten og driften. Detaljert teknisk beskrivelse finnes i hjelpesenteret under Personvern og sikkerhet.

Identitet og tilgang

Tiltak	Detalj
Passord	Argon2id. Minst 12 tegn. Bytte av passord logger ut alle økter
Økter	Kortlevd tilgangstoken (15 minutter) i HttpOnly-cookie og roterende oppdateringstoken (14 dager). Gjenbruk av et rotert token trekker tilbake hele familien
Tofaktor	TOTP, obligatorisk for Leverandørens plattformadministratorer, tilgjengelig for alle voksne brukere. Hemmelighet kryptert med AES-256-GCM
Elever	Ingen passord. Aktivitetskode (6 tegn, 12 timer, kan låses) og personlig kortkode (hash, kan trekkes tilbake)
Autorisasjon	Rolle og nivå avgjøres på serveren ved hver forespørsel. Tenant-id på alle rader. Automatiske tester for scope- og tenantgrenser
Leverandørens tilgang	Ingen innlogging som en annen bruker. All bruk av kundedata fra Leverandøren logges i revisjonsloggen
Hastighetsbegrensning	På innlogging, invitasjoner, kodeoppslag, deltakelse, svar og kontaktskjema

Data

- Fasit lagres på serveren og sendes aldri til elevens nettleser i skoleflyten. Retting skjer deterministisk, uten kunstig intelligens.
- Svar sendes med engangsnøkkel, så nettverksfeil aldri gir dobbeltregistrering.
- Revisjonslogg for rolleendringer, elevadministrasjon, avtaler, eksport, sletting og all bruk av kundedata fra Leverandøren.
- Sletting kjøres som dokumenterte jobber; personidentifikatorer fjernes fysisk.

Transport, lagring og drift

- TLS på all trafikk. Cookies settes Secure i produksjon.
- All behandling og lagring i Hetzners datasenter i Helsinki, Finland: applikasjon, database, mellomlager og sikkerhetskopier. Kryptert lagring og krypterte daglige sikkerhetskopier.
- Ingen hemmeligheter i kildekoden. Konfigurasjon valideres ved oppstart.
- Tilgang til produksjonsmiljøet krever tofaktor og er begrenset til navngitte personer hos Leverandøren.

Logging

Strukturerte logger med request-id. Cookies og autorisasjonshoder maskeres. Feil returneres uten interne detaljer.

Hendelseshåndtering

1. **Oppdag**: alarm, support eller logg.
2. **Vurder**: er personopplysninger berørt, og hvilke kunder.
3. **Begrens**: roter nøkler, trekk tilbake tokens, lås aktiviteter, deaktiver brukere.
4. **Varsle**: Kunden innen 48 timer ved brudd. Kunden varsler Datatilsynet innen 72 timer.
5. **Dokumenter**: tidslinje, omfang, tiltak og læringspunkter.

Universell utforming

Tjenesten utvikles mot WCAG 2.1 AA med automatiske tilgjengelighetstester.

Vedlegg C: Underdatabehandlere og lokasjon

Alle underdatabehandlere er i EU/EØS. Kunden varsles med minst 30 dagers frist før en ny underdatabehandler tas i bruk.

Leverandør	Tjeneste	Data	Lokasjon	Når
Hetzner Online GmbH	Servere for applikasjon, database, mellomlager og sikkerhetskopier	Alle kundedata, kryptert lagring	Datasenter Helsinki, Finland. Ingen kundedata i andre Hetzner-datasentre	Alltid
Cloudflare, Inc.	DNS, beskyttelse mot angrep og kryptert transport foran tjenesten	Trafikkdata i transitt (IP-adresse, forespørsler). Ingen lagring av innhold	Nærmeste datasenter i Cloudflares nettverk, for brukere i Norge normalt Oslo. Ingen lagring; trafikk i transitt for brukere som befinner seg utenfor EU/EØS kan passere lokale Cloudflare-datasentre. EUs standardavtaler (SCC)	Alltid
Resend	Transaksjons-e-post til voksne brukere (invitasjoner, bekreftelser)	Navn, e-post og innholdet i e-posten	EU-regionen (Irland)	Alltid. Aldri e-post til elever
Sikt (Feide)	Innlogging for voksne	Feide-id, navn, organisasjons-id, e-post ved kobling	Norge	Bare kunder som aktiverer Feide
Google	Innlogging og Classroom-import	Voksne: Google-id, e-post, navn. Elever: Google-id og fornavn	Etter Googles Workspace-avtale med Kunden	Bare kunder som aktiverer Google

Egen drift

Supporthenvendelser til hjelp@mattetime.no og fra kontaktskjemaet håndteres i Leverandørens egne systemer for e-post og support, driftet av Leverandøren hos Hetzner i EU.

Ikke i bruk

Annonsenettverk, produktanalyse fra tredjepart, sporingspikslar og chat-verktøy fra tredjepart. Det settes ingen informasjonskapsler ut over dem som trengs for innlogging.

Versjonshistorikk

Versjon	Dato	Endring
1.0	8. september 2026	Første gjeldende versjon. Gjennomgått mot personvernforordningen artikkel 28 nr. 3: plikt til å varsle om ulovlige instruksjer, samme plikter for underdatabehandlere med fullt ansvar hos Leverandøren, innhold i bruddvarsel, bistand ved forhåndsdrøfting, lovvalg og verneting, forrang foran hovedavtalen, kontaktpunkter. Publisert av NiceLab AS etter egen gjennomgang, uten ekstern juridisk bistand.
0.9	8. september 2026	Første publiserte utkast. Datasenter presisert til Hetzner Helsinki for all behandling og lagring. Vedlegg A–C lagt ved.