Sikt
Kunnskapssektorens
tjenesteleverandør

Databehandleravtale for Feide

Behandling av personopplysninger i Feide

Sikt
Kunnskapssektorens tjenesteleverandør

Innholdsfortegnelse

Sikt
Kunnskapssektorens tjenesteleverandør

Databehandleravtale for Feide

Gjeldende versjon av databehandleravtalen for Feide er den som til enhver tid er publisert på Sikts nettsider og erstatter alle tidligere versjoner.

For tilgang til tidligere versjoner, ta kontakt med Sikt på kontakt@sikt.no eller telefon 73 98 40 40.

Materielle endringer som påvirker partenes rettigheter eller plikter varsles Behandlingsansvarlig skriftlig, 30 dager før ikrafttredelse, og endringslogg føres slik at endringer kan etterprøves.

Versjon	Sist oppdatert	Beskrivelse
V. 1.0	16.02.2026	Ferdigstilt DBA for Feide

Generelt

Denne databehandleravtalen fastsetter partenes rettigheter og plikter når Databehandler (Sikt) behandler personopplysninger på vegne av Behandlingsansvarlig (Vertsorganisasjon), som del av leveransen(e) under Avtale om leveranse av Feide, jf. GDPR artikkel 28 nr. 3 bokstav a–h.

Ved motstrid innad i Avtalegrunnlaget for Avtale om leveranse av Feide, har databehandleravtalen forrang når det gjelder forhold spesifikt knyttet til behandling av personopplysninger.

A. Behandlingens art og formål

A.1 Formålet med behandlingen av personopplysninger

Databehandlerens behandling av personopplysninger på vegne av Behandlingsansvarlig er knyttet til å levere tjenester som beskrevet i Avtale om leveranse av Feide.

Behandlingen har følgende hovedformål:

1. **Levere og administrere en sikker innloggings- og datadelingsløsning** som gir enkel og trygg tilgang til digitale tjenester for studenter, forskere og ansatte i utdanning og forskning.

Behandlingen har følgende tilleggsformål:

2. **Tilgangskontroll og tjenestestyring:** Behandle identitets- og tilknytningsopplysninger for å fastsette korrekt tilgangsnivå og å sikre at brukeren mottar riktig tjenestetilpasning fra sin vertsorganisasjon.
3. **Operativ drift:** Behandle teknisk driftsdata for å sikre stabil og effektiv levering av Feide-tjenester, herunder feilsøking, overvåking av oppetid og opprettholdelse av teknisk kvalitet.
4. **Sikkerhetsformål**: For å kunne identifisere og avdekke sikkerhets- eller misbrukshendelser, med formål å utlevere hendelsesdata og logger til Behandlingsansvarlig.

Sikt er behandlingsansvarlig for følgende formål:

5. **Sikkerhetsformål**: For å kunne identifisere og avdekke sikkerhets- eller misbrukshendelser hos en Behandlingsansvarlig eller på tvers av Behandlingsansvarlige, med formål å informere samt utlevere hendelsesdata og logger ved behov til berørte Behandlingsansvarlige.
6. **Videreutvikling og forbedring av tjenesten**: For å analysere aggregert bruksstatistikk med sikte på å forbedre Feides funksjonalitet og brukeropplevelse.
7. **Kundeoppfølging og administrasjon**: For å behandle kontaktopplysninger og organisasjonsdata i forbindelse med administrasjon av kundeforholdet, inkludert utsendelse av driftsvarsler, endringsmeldinger og annen nødvendig informasjon relatert til tjenesten.
8. **Statistikk til sektorformål**: For å utarbeide aggregert statistikk om bruk av Feide, til forskningsformål for nasjonale utdanningsmyndigheter, lovpålagte myndighetsoppgaver og for å besvare forespørsler fra Riksrevisjonen.

For formål hvor Sikt er behandlingsansvarlig bestemmer Sikt hvorfor og hvordan opplysningene brukes.

For øvrig vises det til Feides personvernerklæring (https://www.feide.no/personvernerklaering) for nærmere opplysninger om denne behandlingen.

Behandlingen pågår så lenge Avtale om leveranse av Feide er i kraft, og avsluttes i henhold til pkt. A.4.

Sikt
Kunnskapssektorens tjenesteleverandør

A.2 Behandlingens art

Databehandlerens behandling av personopplysninger på vegne av Behandlingsansvarlig omhandler (arten av behandling), inkludert følgende personopplysninger:

Behandlingsaktivitet	Spesifikasjon	Formål	Hvilke opplysninger	Varighet
Innlogging i tjenesten Innhenting av relevant data Registrering i kundeportalen	Deling av informasjon fra vertsorganisasjonenes register, tilgjengelig i Feides brukerkatalog.	• Levere og administrere Feide, herunder tilpasning av tjenesten. • Tilgangskontroll • Operativ drift • Kommunikasjon	• Navn • Fødselsnummer • Brukernavn • Feide-ID • Kontaktinformasjon • Organisasjonstilknytning • Gruppetilhørighet (emne, klasse) • Foresatte for elever i grunnopplæringen • Relevant Feide-tjeneste • Rettighet knyttet til rolle som administrator • Aktivitets- og bruksdata	Personopplysninger behandles så lenge Feide er i bruk, og slettes ellers etter 180 dager.
Logging	Logging på vegne av kunder	Sikkerhetsformål	• IP-adresse • Brukernavn • Feide-ID • Nettleser • Aktivitetsdata	180 dager

A.3 Kategorier av registrerte

Behandlingen omfatter følgende kategorier av registrerte:

- Elever i grunnskolen og videregående skole
- Studenter i høyere utdanning
- Lærere og forelesere
- Øvrige med tilknytning til Behandlingsansvarlig

A.4 Varighet av behandlingen

Databehandlers behandling av personopplysninger er ikke tidsbegrenset og varer frem til opphør av Avtale om leveranse av Feide.

Ved opphør av Avtale om leveranse av Feide skal alle personopplysninger som behandles på vegne av Behandlingsansvarlig, samt eventuell annen relevant informasjon etter Behandlingsansvarliges instruks, tilbakeleveres eller slettes.

Etter gjennomført tilbakelevering plikter Databehandler å slette alle gjenværende personopplysninger og relevant informasjon som behandles på vegne av Behandlingsansvarlig, innen 30 dager, med mindre videre lagring er påkrevd etter lov.

Sikt
Kunnskapssektorens tjenesteleverandør

B. Godkjente underdatabehandlere

B.1 Oversikt over underdatabehandlere

Den Behandlingsansvarlige har godkjent bruk av følgende underdatabehandlere:

Navn	Lokasjon	Kontaktopplysninger	Beskrivelse av behandlingen	Behandlingssted
Amazon Web Services (AWS Europe)	USA	tbalvig@amazon.com (+4551800679) David.degroot@rackspace.com (+31612729675) Parvez.hussain@rackspace.com	Benyttes gjennom GEANTs LaaS – rammeavtale med Rackspace for å levere all kjernefunksjonalitet i Feide, eks. innlogging, tilgangskontroll til APIer samt APIer Feide leverer. I tillegg benyttes AWS til de fleste støttetjenester i Feide, for eksempel kundeportal, datakvalitetssjekker o.l. **Personopplysninger**: Navn Fødselsnummer Brukernavn Feide-ID Kontaktinformasjon Organisasjonstilknytning Gruppetilhørighet (emne, klasse) Foresatte for elever i grunnopplæringen Relevant Feide-tjeneste Rettighet knyttet til rollen som Feide-administrator Aktivitets- og bruksdata	EU/EØS Overføringsgrunnlag: DPF
Telenor Norge	Norge	Org.nr.: 976 967 631 Strandgaten 9, 7900 Rørvik	Benyttes til utsending av engangskoder ved pålogging for de som bruker SMS til sterk autentisering. **Personopplysninger**: Telefonnummer	EØS
Telia AS	Norge	Org. nr.: 7981 929055 Lørenfart 1, 0580 Oslo	Benyttes til utsendelse av engangskode ved pålogging for de som bruker SMS til sterk autentisering. **Personopplysninger**: Telefonnummer	EØS

B.2 Behandlingsansvarliges godkjennelse

Databehandler har Behandlingsansvarliges generelle godkjennelse til å benytte overnevnte underdatabehandlere. Databehandler skal likevel skriftlig underrette Behandlingsansvarlig om planer om å erstatte eller engasjere nye underdatabehandlere.

Slik underretning skal gis minimum 30 dager før endringen trer i kraft, med mindre endringen er akutt nødvendig for å sikre opprettholdelse av leveranse av avtalt tjeneste.

Dersom Behandlingsansvarlig motsetter seg endringen, må dette meddeles Databehandler senest 14 dager etter mottatt underretning.

Ved en ekstraordinær situasjon som krever umiddelbare tiltak for å sikre tilgjengelighet eller informasjonssikkerhet i tjenesten, kan Databehandler uten forhåndsvarsel fjerne, erstatte eller engasjere underdatabehandler. Behandlingsansvarlig skal varsles skriftlig uten ugrunnet opphold, og senest innen 7 (syv) virkedager etter endringen.

C. Tekniske, organisatoriske og sikkerhetsmessige tiltak

C.1 Sikkerhet ved behandlingen

Databehandler plikter å treffe og gjennomføre tekniske, organisatoriske og sikkerhetsmessige tiltak slik at det til enhver tid er et sikkerhetsnivå som er egnet med hensyn til risiko ved behandling av personopplysninger, jf. GDPR artikkel 32.

Behandlingsansvarlig kan kontakte Sikt for en uttømmende og oppdatert oversikt over alle tekniske og organisatoriske sikkerhetstiltak til bruk i Feide.

Sikt
Kunnskapssektorens
tjenesteleverandør

Eksempel på sikkerhetstiltak på bruk i Feide:

Informasjonssikkerhetsstyring	Informasjonssikkerhetsstyringssystem basert på ISO/IEC 27001:2013, gjennomføring av risikovurderinger og etablert sikkerhetsteam i Sikt, herunder også eduCSC.
Tilgangskontroll og autentisering	Begrenset og kontrollert tilgang for operativt personell, kraft til MFA for alle tilganger, og overvåkning av alle tilganger til underliggende infrastruktur.
Infrastruktur- og nettverkssikkerhet	Nettverkssegmentering og bruk av ACLs/security groups med «default deny», versjonskontroll og overvåkning av sikkerhetskonfigurasjoner, samt bruk av infrastruktur som kode (IaC) og automasjon for konsistent og sikker konfigurasjon, patching og drift.
Kryptering	Kryptering av all data i transit med moderne TLS-konfigurasjoner og offentlige sertifikater, samt kryptering av data lagret i offentlige skymiljøer ved bruk av tjenestespesifikke nøkler.
Sikker utviklings- og driftsprosess	Statisk kodeanalyse, sårbarhetsskanning av avhengigheter og containerbilder, obligatorisk kodegjennomgang, automatiserte tester i CI/CD og bruk av dedikerte løsninger for sikker håndtering av hemmeligheter.
Overvåking og hendelseshåndtering	Sentralisert logging og monitorering med nær sanntidsvarsling, etablerte prosesser for hendelseshåndtering inkludert kriseeskalering, og tilgjengelig rapporteringsmulighet 24/7 via Sikt Servicesenter.
Tilgjengelighet og gjenoppretting	Redundant tjenestearkitektur, automatisk skalering basert på belastning, samt daglige sikkerhetskopier lagret separat fra produksjonsmiljø og kryptert med tjenestespesifikke nøkler.
Eksterne sikkerhetsvurderinger	Bruk av eksterne sikkerhetskonsulenter til vurderinger og penetrasjonstester av tjenester og sentrale komponenter, herunder gjennomganger av SimpleSAMLphp-kodebasen.

D. Rettigheter og plikter

D.1 Behandlingsansvarliges plikter og rettigheter

Behandlingsansvarlig har ansvar for at behandlingen av personopplysninger skjer i samsvar med GDPR, jf. artikkel 24.

Behandlingsansvarlig har rett og plikt til å sørge for at:

1. Behandlingen av personopplysninger er formålsbestemt og basert på et gyldig behandlingsgrunnlag, jf. GDPR kapittel 2.
2. Formålet med behandlingen og hvilke hjelpemidler som kan benyttes, fastsettes av Behandlingsansvarlig i samsvar med GDPR artikkel 4 nr. 7.
3. Databehandler kun behandler personopplysninger i samsvar med de dokumenterte instruksene som gis av Behandlingsansvarlig og ellers i tråd med overnevnte formål, jf. GDPR artikkel 28 nr. 3 bokstav a).
4. Eventuelle endringer i instruksen skal varsles til Databehandler, som implementerer endringene innen rimelig tid. Databehandler kan kreve at Behandlingsansvarlig dekker dokumenterte kostnader som påløper i forbindelse med implementeringen av slike endringer eller forholdsmessig justering av vederlaget dersom instruksen medfører løpende ekstra kostnader. Det samme gjelder merkostnader som følge av endringer i GDPR, som følge av Behandlingsansvarliges virksomhet.

D.2 Databehandlers rettigheter og plikter

Databehandler har rett og plikt til å sørge for at:

1. Personopplysninger kun behandles i samsvar med dokumenterte instrukser fra Behandlingsansvarlig; dersom Databehandler er rettslig forpliktet til å avvike fra instruksen, skal Behandlingsansvarlig varsles før behandlingen, med mindre loven forbyr slik varsling, jf. GDPR artikkel 28 nr. 3 bokstav a).
2. Kun autoriserte personer gis tilgang til personopplysningene, at slike personer er underlagt taushetserklæring eller lovbestemt taushetsplikt, at tilgang fjernes når autorisasjon faller bort, og at Databehandler på anmodning kan dokumentere at krav til konfidensialitet og integritet er oppfylt; plikten til konfidensialitet gjelder også etter oppdragets opphør.
3. Databehandler skal dokumentere de rutiner og tiltak som er iverksatt for å oppfylle kravene som følger av GDPR og Databehandleravtalen. Slik

dokumentasjon skal oppbevares og ajourholdes så lenge Databehandleravtalen består, og gjøres tilgjengelig for Behandlingsansvarlig eller tilsynsmyndigheter på forespørsel.

4. Gjøre tilgjengelig for Behandlingsansvarlig all informasjon som er nødvendig for å påvise at Databehandlers forpliktelser fastsatt i GDPR artikkel 28 og forpliktelser under Avtale om leveranse av Feide er oppfylt.
5. Eventuelle underdatabehandlere kun engasjeres gjennom skriftlig avtale som pålegger underdatabehandlere de samme forpliktelsene som følger av denne Databehandleravtalen. Databehandler står fullt ansvarlig overfor Behandlingsansvarlig dersom en underdatabehandler ikke oppfyller sine plikter, jf. GDPR artikkel 28 nr. 3 bokstav d).
6. Databehandler skal, tatt i betraktning behandlingens art og informasjonen Databehandler har tilgjengelig, bistå Behandlingsansvarlig med å oppfylle sine forpliktelser etter GDPR artikkel 32–36, herunder ved vurderinger av personvernkonsekvenser (DPIA) og eventuelle forhåndsdrøftinger med tilsynsmyndigheten.
7. Databehandler skal, så langt det er mulig og hensiktsmessig, bistå Behandlingsansvarlig med å besvare henvendelser fra registrerte om deres rettigheter etter GDPR kapittel 3.
8. Databehandler skal uten ugrunnet opphold videreformidle eventuelle henvendelser fra registrerte til Behandlingsansvarlig, og skal ikke svare direkte på slike henvendelser uten skriftlig instruks fra Behandlingsansvarlig, jf. GDPR artikkel 28 nr. 3 bokstav e).
9. Personopplysninger tilbakeleveres eller slettes ved opphør av avtaleforholdet, i samsvar med Behandlingsansvarliges instruks, jf. GDPR artikkel 28 nr. 3 bokstav g).
10. Databehandler skal gjøre tilgengelig all informasjon som er nødvendig for at Behandlingsansvarlig kan påvise at forpliktelsene fastsatt i GDPR artikkel 28 er oppfylt, samt muliggjør og bidra til revisjon som beskrevet i GDPR artikkel 28 nr. 3 bokstav h).
11. Databehandler skal omgående underrette den Behandlingsansvarlige dersom vedkommende mener at instruksene er i strid med gjeldende personvernregler, jf. GDPR artikkel 28 nr. 3 andre avsnitt.
12. Eventuelle endringer i instruks skal varsles til Databehandler som implementerer endringene innen rimelig tid. Databehandler kan kreve at Behandlingsansvarlig dekker dokumenterte kostnader som påløper i forbindelse med implementeringen av slike endringer eller forholdsmessig justering av vederlaget under Avtale om leveranse av Feide dersom den endrede instruksen innebærer

løpende ekstra kostnader for Databehandleren. Det samme gjelder merkostnader som følge av endringer av Gjeldende personvernregler som gjelder den Behandlingsansvarliges virksomhet.

13. Det etableres egnede tekniske og organisatoriske tiltak for å oppnå et egnet sikkerhetsnivå, jf. GDPR artikkel 32.

E. Melding om brudd på personopplysningssikkerheten

Databehandler skal uten ugrunnet opphold skriftlig underrette den Behandlingsansvarlige om brudd på personopplysningssikkerheten, samt gi slik bistand og informasjon som er nødvendig for at den Behandlingsansvarlige skal kunne gi melding til Datatilsynet.

Ved omfattende brudd på personopplysningssikkerheten, vil Databehandler varsle Datatilsynet innen 72 timer, jf. GDPR artikkel 33. Databehandler vil underrette Behandlingsansvarlig om varselet omgående.

I varsel vil Databehandler oppgi tilgjengelig informasjon om art og omfang av bruddet, herunder hvilke Behandlingsansvarlige som er berørte.

Databehandlers varsel fritar ikke Behandlingsansvarlig fra å gjøre en selvstendig vurdering av om det er nødvendig å gi Datatilsynet ytterligere informasjon, og å underrette de registrerte om brudd på personopplysningssikkerheten jf. GDPR artikkel 33 nr. 4 og artikkel 34.

F. Revisjon

Dersom en revisjon avdekker avvik fra forpliktelsene i gjeldende personvernregler eller Avtale om leveranse av Feide, skal Databehandler uten ugrunnet opphold utbedre avviket. Behandlingsansvarlig kan kreve at Databehandler midlertidig stopper hele eller deler av behandlingsaktivitetene frem til utbedring er godkjent av Behandlingsansvarlig.

Hver av Partene dekker sine egne kostnader forbundet med inspeksjoner fra aktuelle tilsynsmyndigheter og inntil én årlig revisjon initiert av Behandlingsansvarlig. Hvis en revisjon avdekker vesentlige brudd på forpliktelsene etter gjeldende personvernregler eller Avtale om leveranse av Feide, skal Behandlingsansvarlig likevel dekke Databehandlers rimelige kostnader forbundet med revisjonen.