

DATABEHANDLERAVTALE

FOR DIGITALE LEVERANSER TIL NASJONAL DATABASE FOR GRUNNUNDERSØKELSER (NADAG)



Er inngått mellom:

Norges geologiske undersøkelse (NGU), organisasjonsnummer: NO 970 188 290

heretter kalt Databehandler

og dataleverandøren

<Angi navn på virksomhet> og <organisasjonsnummer>

heretter kalt Behandlingsansvarlig

I fellesskap kalt Partene.

Sted og dato

<sted>, <dato>

Avtalen er signert elektronisk.

Avtaleparter

<behandlingsansvarlig virksomhet>

<Navn>

Norges geologiske undersøkelse

May Britt Myhr

[Signatur behandlingsansvarlig]

[Signatur databehandler]

Bilag

1. Informasjon om behandlingen av personopplysninger
2. Tekniske og organisatoriske tiltak

I tråd med personvernforordningen artikkel 28 (3) inngås denne Databehandleravtalen i forbindelse med plikten til å melde inn og tilgjengeliggjøre data og rapporter etter pbl. § 2-4¹ og tilhørende forskrift², gjennom tjenesten Nasjonal database for grunnundersøkelser (NADAG)³, i tillegg til frivillig innmelding av data innsamlet før loven trådte i kraft.

Ved oppdatering av eller endringer i Databehandleravtalen skal Partene informere motparten skriftlig per e-post innen 30 dager før endringene trer i kraft. Eventuelle endringer skal godkjennes skriftlig av Behandlingsansvarlig.

En oppdatert tjenestebeskrivelse av NADAG er tilgjengelig på NGUs nettsider⁴.

1. Formålet med denne Databehandleravtalen

Denne avtalen («Databehandleravtalen») fastsetter partenes rettigheter og plikter når Databehandleren behandler personopplysninger på vegne av den Behandlingsansvarlige som del av tjenesten. Databehandleravtalen har som formål å sikre at Partene etterlever gjeldende personvernregler⁵.

2. Omfang

Databehandleren gis rett til å behandle personopplysninger på vegne av Behandlingsansvarlig i henhold til vilkår og betingelsene i Databehandleravtalen.

Databehandleren kan kun behandle personopplysninger underlagt denne Databehandleravtalen. Alle personopplysninger som behandles av Databehandler på vegne av Behandlingsansvarlig under denne avtalen vil bli referert til som «personopplysningene».

Bilag 1 til denne Databehandleravtalen inneholder en nærmere beskrivelse av behandlingen som skal foretas, herunder om behandlingsformål, kategorier av personopplysninger og registrerte, regler for sletting og tilbakelevering, og Partenes kontaktpersoner.

Bilag 2 til denne Databehandleravtalen inneholder opplysninger om tekniske og organisatoriske tiltak.

3. Behandlingsansvarliges plikter

Behandlingsansvarlig har ansvaret for at behandlingen av personopplysninger skjer i samsvar med gjeldende personvernregler. Behandlingsansvarlige skal i den forbindelse særskilt sørge for at:

- i. behandlingen av personopplysninger er formålsbestemt og basert på et gyldig rettsgrunnlag;
- ii. de registrerte har mottatt nødvendig informasjon om behandlingen av personopplysningene;
- iii. behandlingsansvarlig har gjennomført tilstrekkelige risikovurderinger;
- iv. databehandler til enhver tid har tilstrekkelig informasjon for å oppfylle sine plikter i henhold til Databehandleravtalen og gjeldende personvernregler;
- v. behandlingsansvarlig til enhver tid har kontroll og autoritet over personopplysningene; og at datatilsynet og berørte registrerte blir informert ved eventuelle brudd på personopplysnings-sikkerheten, se punkt 4.4.

¹ <https://lovdata.no/LTI/lov/2024-06-21-52>

² <https://lovdata.no/LTI/forskrift/2024-12-17-3181>

³ [Nasjonal database for grunnundersøkelser](#)

⁴ [Om NADAG - Nasjonal database for grunnundersøkelser | NGU](#)

⁵ Den til enhver tid gjeldende versjon av EUs personvernforordning (2016/679), samt lov om behandling av personopplysninger av 15.06.2018 med tilhørende forskrifter mv., samt eventuell annen relevant lovgivning som gjelder behandling og vern av personopplysninger.

4. Databehandlerens plikter

4.1. Generelle plikter

Databehandleren skal behandle personopplysningene i samsvar med gjeldende personvernregler. Hvis annen behandling er nødvendig for å oppfylle forpliktelse som Databehandler er underlagt i henhold til gjeldende rett, skal Databehandleren underrette den Behandlingsansvarlige så langt dette er tillat ved lov, jf. personvernforordningen artikkel 28 (3), bokstav (a).

Databehandleren skal imøtekomme pålegg fra Behandlingsansvarlig om å slette eller returnere alle personopplysninger (inkludert kopier) etter at tjenestene knyttet til behandlingen er avsluttet, med mindre lovkrav pålegger lagring, jf. personvernforordningen artikkel 28 (3), bokstav (g). Personopplysninger som kan komme frem av innmeldte rapporter og utredninger er omfattet av lovkrav som pålegger lagring (pbl. § 2-4).

4.2. Tekniske og organisatoriske tiltak

Databehandler skal iverksette egnede tekniske og organisatoriske tiltak for å oppnå et tilfredsstillende sikkerhetsnivå sett hen til behandlingens karakter og omfang, den tekniske utviklingen, implementeringskostnader og aktuelle risikoer for fysiske personers rettigheter og friheter. Databehandleren skal som minimum iverksette de tiltak som er spesifisert i Databehandleravtalens **Bilag 2**.

Databehandleren skal foreta risikovurderinger for å sikre at et egnet sikkerhetsnivå opprettholdes til enhver tid. Databehandleren skal herunder sørge for jevnlig testing, analyse og vurdering av sikkerhetstiltakene, særlig med hensyn til å sikre vedvarende konfidensialitet, integritet, tilgjengelighet og robusthet i behandlingssystemer og -tjenester, samt evne til raskt å gjenopprette tilgjengeligheten av personopplysningene ved hendelser.

Databehandler skal dokumentere risikovurderingen og sikkerhetstiltakene, og gjøre dem tilgjengelig for Behandlingsansvarlige på forespørsel.

4.3. Konfidensialitet og taushetsplikt

Databehandleren skal kun autorisere personer som trenger tilgang til personopplysningene i forbindelse med arbeid for å kunne utføre tjenesten, Databehandleravtalen og eventuelt annen behandling som er nødvendig for å oppfylle forpliktelser som Databehandler er underlagt i henhold til gjeldende personvernregler.

Databehandleren skal sikre at ansatte og andre som har tilgang til personopplysninger er autorisert til å behandle slike personopplysninger på Databehandlers vegne. Dersom slik autorisasjon utløper eller trekkes tilbake, skal tilgangen til personopplysningene opphøre uten ugrunnet opphold.

Databehandleren skal sikre at personer som er autorisert til å behandle personopplysninger på vegne av den Behandlingsansvarlige er underlagt taushetsplikt gjennom avtale eller lov. Taushetsplikten skal bestå også etter avtalens og/eller ansettelsesforholdets opphør, og kunne dokumenteres på forespørsel fra Behandlingsansvarlig.

Ved opphør av Databehandleravtalen plikter Databehandler å avvikle alle tilganger til personopplysninger som behandles under denne avtalen. Se også punkt 8 og 9 i denne avtalen.

4.4. Sikkerhetsbrudd

Databehandleren skal varsle Behandlingsansvarlig om ethvert brudd på personopplysningssikkerheten som potensielt kan føre til utilsiktet eller ulovlig ødeleggelse, endring, uautorisert utlevering av eller tilgang til personopplysninger. Sikkerhetsbrudd må rapporteres til Behandlingsansvarlig uten ugrunnet

opphold etter at Databehandler har mistanke om avviket, selv om Databehandleren ikke har all nødvendig informasjon tilgjengelig. Melding til Behandlingsansvarlig om eventuelle avvik skal ikke utsettes i påvente av undersøkelser av årsak, omfang og konsekvenser.

Etter å ha mottatt rapport om sikkerhetsbrudd, er Behandlingsansvarlig ansvarlig for å informere den eller de berørte personene samt melde bruddet til Datatilsynet i tråd med gjeldende personvernregler. Databehandler skal ikke informere tredjeparter om brudd på personopplysningssikkerheten med mindre noe annet er påkrevd etter gjeldende rett.

Ved underretning om sikkerhetsbrudd til Behandlingsansvarlig skal Dataansvarlig:

- beskrive arten av bruddet på personopplysningssikkerheten, herunder, når det er mulig, kategoriene av og omtrentlig antall registrerte som er berørt, og kategoriene av og omtrentlig antall registreringer av personopplysninger som er berørt,
- inneholde navnet på og kontaktopplysninger til personvernombudet eller annet kontaktpunkt der mer informasjon kan innhentes,
- beskrive de sannsynlige konsekvensene på bruddet på personopplysningssikkerheten, og
- beskrive de tiltak som Databehandleren har truffet eller foreslår å treffe for å håndtere bruddet på personopplysningssikkerheten, herunder, dersom det er relevant, tiltak for å redusere eventuelle skadevirkninger som følge av bruddet.

Ovennevnte informasjon kan i den grad det er nødvendig gis trinnvis uten ytterligere ugrunnet opphold.

Databehandler plikter å gjennomføre alle de tiltak som med rimelighet kan kreves for å utbedre og unngå tilsvarende brudd på personopplysningssikkerheten. Databehandler skal, så langt det er mulig, rådføre seg med Behandlingsansvarlig om de tiltak som skal gjennomføres, herunder vurdere Behandlingsansvarliges eventuelle forslag til tiltak.

4.5. Bistand til behandlingsansvarlig

Databehandleren skal på forespørsel bistå Behandlingsansvarlig med oppfyllelse av de registrertes rettigheter etter personvernforordningens kapittel III gjennom egnede tekniske eller organisatoriske tiltak. Plikten til å bistå gjelder likevel bare i den utstrekning dette er mulig og hensiktsmessig sett hen til karakteren og omfanget av behandlingen av personopplysninger for å utføre tjenesten.

Databehandleren skal bistå den Behandlingsansvarlige med å overholde kravene til personopplysningssikkerhet i personvernforordningen artikkel 32-36.

Databehandler skal uten ugrunnet opphold videresende alle henvendelser som Databehandler eventuelt mottar fra den registrerte vedrørende den registrertes rettigheter i henhold til gjeldende personvernregler til Behandlingsansvarlig. Slike henvendelser kan kun besvares av Databehandler når dette er skriftlig godkjent av Behandlingsansvarlig.

Behandlingsansvarlig skal gi slik bistand og informasjon som er nødvendig for at Behandlingsansvarlig ved sikkerhetsbrudd kan informere berørte personer og melde bruddet til Datatilsynet.

5. Bruk av underleverandører

Databehandler kan benytte underleverandører for behandling av personopplysninger etter denne Databehandleravtalen i forbindelse med drift og vedlikehold av tjenestene.

Databehandler og underleverandører skal inngå en skriftlig avtale som pålegger disse tilsvarende forpliktelser med hensyn til vern av personopplysninger som Databehandleren selv er underlagt etter denne Databehandleravtalen. På forespørsel av Behandlingsansvarlig skal Databehandler forelegge en oversikt over godkjente underleverandører og de delene av avtaler med underleverandører som er relevant for behandlingen av personopplysninger.

Databehandler er ansvarlig for underleverandørens utførelse av oppgaver for Databehandler, på samme måte som om Databehandler er ansvarlig for selve utførelsen. Underleverandøren skal gjennomføre egnede tekniske og organisatoriske tiltak som sikrer at behandlingen oppfyller kravene etter gjeldende personvernregler. Databehandler skal gjennomføre kontroller for å verifisere tiltakene hos underleverandør, og kunne forelegge rapporter fra slike kontroller for Behandlingsansvarlig på forespørsel.

6. Overføring av personopplysninger til land utenfor EØS

Personopplysninger som Databehandler eller underleverandører behandler, kan bare overføres til land utenfor EØS-området eller til en internasjonal organisasjon, hvis Behandlingsansvarlig skriftlig har godkjent slik overføring, og vilkårene for beskyttelsesnivå for personvern etter gjeldende personvernregler⁶ er oppfylt.

Databehandler kan likevel overføre personopplysninger dersom dette kreves i henhold til gjeldende rett i EØS-området. Databehandler skal underrette Behandlingsansvarlig om slik overføring så langt dette er tillat ved lov.

7. Inspeksjoner og revisjoner

Behandlingsansvarlig har rett til, etter samråd med Databehandleren, å foreta inspeksjoner eller å få dem utført av en revisor, for å påvise at forpliktelsene fastsatt i gjeldende personvernregler og at denne Databehandleravtalen er oppfylt.

Behandlingsansvarlig skal varsle Databehandler i rimelig tid før en revisjon finner sted. Innenfor ordinær arbeidstid kan Behandlingsansvarlig foreta uanmeldte stikkprøver for å sikre seg at forpliktelsene etter denne avtalen overholdes. Databehandler skal muliggjøre og bidra ved inspeksjoner og revisjoner, enten de gjennomføres av eller i oppdrag av Behandlingsansvarlig, eller av aktuelle tilsynsmyndigheter. Tilsyn med eventuelle underleverandører skal skje gjennom Databehandleren med mindre annet er særskilt avtalt.

Databehandler skal sørge for at all informasjon som er nødvendig for å påvise at forpliktelsene fastsatt i gjeldende personvernregler og denne avtalen er oppfylt, gjøres tilgjengelig for Behandlingsansvarlig ved forespørsel.

Dersom det ved inspeksjon eller revisjon avdekkes avvik fra forpliktelsene i gjeldende personvernregler eller Databehandleravtalen, skal Databehandler så snart som mulig utbedre avviket. Behandlingsansvarlig kan kreve umiddelbar stans i hele eller deler av behandlingsaktivitetene frem til utbedringer er godkjent av Behandlingsansvarlig.

8. Mislighold, varighet og opphør

Databehandleravtalen gjelder fra den er signert av begge Parter. Databehandleravtalen gjelder så lenge Databehandler behandler personopplysninger på vegne av Behandlingsansvarlig. Den gjelder også for eventuelle personopplysninger som måtte finnes hos Databehandler eller noen av dennes underleverandører etter tjenestens opphør.

Databehandleravtalen kan ikke sies opp så lenge tjenesten og innmeldingsplikten jf. pbl. § 2-4 består og Behandlingsansvarlig produserer data som er omfattet av innmeldingsplikten, eller melder inn data innsamlet før loven trådte i kraft.

⁶ Jf. personvernforordningen artikkel 45, 46 (2) c eller bindende virksomhetsregler iht. artikkel 47

Databehandleravtalen opphører når dataleverandøren ikke lenger er omfattet av innmeldingsplikten jf. pbl. § 2-4, eller heller ikke lenger skal melde inn data innsamlet før loven trådte i kraft, og dermed ikke lenger er Behandlingsansvarlig, f.eks. ved konkurs, fusjon eller annen virksomhetsendring. Behandlingsansvarlig skal underrette Databehandler om slike endringer.

Revisjon av Databehandleravtalen er ikke opphør.

Ved brudd på Databehandleravtalen og/eller gjeldende personvernregler, kan Behandlingsansvarlig og aktuelle tilsynsmyndigheter pålegge Databehandler å stoppe hele eller deler av behandlingen av opplysningene med øyeblikkelig virkning.

9. Sletting og tilbakelevering av opplysninger

Ved opphør av denne Databehandleravtalen plikter Databehandler å slette alle personopplysninger som behandles på vegne av Behandlingsansvarlig under Databehandleravtalen. Dette gjelder også eventuelle sikkerhetskopier. Dette gjelder ikke personopplysninger som kan komme frem av innmeldte rapporter og utredninger.

Hvis det benyttes delt infrastruktur eller sikkerhetskopi der direkte sletting ikke er teknisk mulig, skal Databehandler sørge for at personopplysningene gjøres utilgjengelige inntil de er overskrevet.

Databehandler skal bekrefte skriftlig overfor Behandlingsansvarlig at sletting eller utilgjengeliggjøring er foretatt og skal på forespørsel dokumentere hvordan det er gjennomført.

Nærmere bestemmelser om sletting fremgår av **Bilag 1**.

10. Lovvalg og verneting

Avtalen er underlagt norsk rett. Verneting er Oslo.

Bilag 1 Informasjon om behandlingen av personopplysninger

a) Omfang og formålet med behandlingen av personopplysninger

Databehandlerens behandling av personopplysninger på vegne av Behandlingsansvarlig er knyttet til å levere tjenesten Nasjonal database for grunnundersøkelser (NADAG) som beskrevet på NGUs nettsider⁷ og for de formål som er beskrevet i Databehandleravtalen med bilag.

Behandlingen har følgende formål:

- Melde inn og tilgjengeliggjøre data og rapporter etter pbl. § 2-4 (rettslig forpliktelse).

Databehandlerens behandling av personopplysninger på vegne av den Behandlingsansvarlige omhandler registrering, organisering og oppbevaring av nødvendige personopplysninger for å kunne identifisere medarbeidere hos den Behandlingsansvarlige som har anledning til å melde inn data til NADAG. Personopplysninger som kan komme fram av innmeldte rapporter er omfattet av databehandlingen der lovkrav pålegger lagring, jf. personvernforordningen artikkel 28 (3), bokstav (g), og blir offentlige etter innmelding.

Databehandler har ikke råderett over personopplysningene utover det som er nødvendig for å oppfylle sine plikter etter Databehandleravtalen, og kan ikke behandle disse til egne formål.

Behandlingen omfatter ingen personopplysninger innenfor særlige kategorier (GDPR ar. 9 (1)) eller andre opplysninger med særlig behov for beskyttelse.

b) Sikkerhet ved behandlingen

Databehandlingen krever ikke et høyt sikkerhetsnivå. Behandlingen omfatter begrensede personopplysninger knyttet til Behandlingsansvarliges brukerprofil (navn, fødselsnummer, e-post, telefonnummer og firmatilhørighet) og til selve leveransen (navn, e-post). Sistnevnte kan finnes i innmeldte dokumenter (som regel pdf-format).

Databehandleren skal ha et egnet styringssystem for informasjonssikkerhet. Databehandleren skal etablere og forvalte tilstrekkelige tekniske og organisatoriske sikkerhetstiltak for å ivareta informasjonssikkerheten for behandling av personopplysningene. Disse tiltakene er beskrevet i **bilag 2**.

c) Dokumentasjon

Databehandler skal dokumentere de rutiner og tiltak som er iverksatt for å oppfylle kravene som fremkommer av gjeldende personvernregler og Databehandleravtalen, herunder kravene til informasjonssikkerhet.

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

d) Overføring av personopplysninger - lokasjon for behandling og tilgang

Behandling av personopplysninger som avtalen omfatter kan ikke uten Behandlingsansvarliges skriftlige godkjenning utføres på eller med tilgang fra andre steder enn fra Databehandler og eventuelle underleverandører. Personopplysninger som kan komme fram i innmeldte rapporter er offentlig tilgjengelig.

Databehandleren skal på forespørsel fra den Behandlingsansvarlige redegjøre for hvor personopplysningene til enhver tid behandles.

⁷ [Om NADAG - Nasjonal database for grunnundersøkelser | NGU](#)



e) Rutiner for revisjon og tilsyn/inspeksjon

For å kontrollere etterlevelse av gjeldende personvernregler og Databehandleravtalen er det avtalt følgende:

Behandlingsansvarlig har rett til å utføre revisjon hos Databehandleren for å verifisere Databehandlerens etterlevelse av sine plikter i henhold til databehandleravtalen eller gjeldende personvernregler.

Slike revisjoner kan gjennomføres etter rimelig forhåndsvarsel og maksimalt én gang i året.

f) Varighet, sletting og tilbakelevering av personopplysninger

Behandlingen varer så lenge Databehandler behandler personopplysninger på vegne av Behandlingsansvarlig, og NGU er registermyndighet for grunnundersøkelser etter forskrift⁸.

Partene har avtalt følgende om sletting av personopplysninger:

Alle personopplysninger som behandles under Databehandleravtalen skal slettes uten ugrunnet opphold og senest innen 90 kalenderdager etter opphør av Databehandleravtalen. Det samme gjelder eventuell annen relevant informasjon som forvaltes på vegne av Behandlingsansvarlig.

g) Kontaktinformasjon

Ved henvendelser i henhold til denne avtalen, eksempelvis ved varsling om brudd på personopplysningssikkerheten eller endring i bruk av underleverandører, skal følgende kanaler benyttes:

Hos Databehandler

Sikkerhetsbrudd personvern:

E-post: personvernombud@ngu.no

Andre henvendelser:

E-post: ngu@ngu.no

Telefon: 73 90 40 00

Hos Behandlingsansvarlig

Sikkerhetsbrudd personvern:

Navn/rolle: [Fyll ut]

Telefon: [Fyll ut]

E-post: [Fyll ut]

Andre henvendelser:

Navn/rolle: [Fyll ut]

Telefon: [Fyll ut]

E-post: [Fyll ut]

⁸ <https://lovdata.no/LTI/forskrift/2024-12-17-3181>



Bilag 2 Tekniske og organisatoriske tiltak

Databehandler skal gjennomføre egnede tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som er tilpasset hensynet til risiko. Dette gjelder også sikkerhetstiltak som brukes for å beskytte personopplysninger i samsvar med gjeldende lovverk, da især GDPR. Hvilke tiltak som er aktuelle vil være avhengig av avtalens beskaffenhet og tekniske og organisatoriske egenskaper.

Databehandleren skal ha et egnet styringssystem for informasjonssikkerhet. Databehandleren skal etablere og forvalte tilstrekkelige tekniske og organisatoriske sikkerhetstiltak for å ivareta informasjonssikkerheten for behandling av personopplysningene, knyttet til følgende punkter:

Tekniske tiltak:

- Kryptering
- Tilgangskontroll
- Systemovervåking
- Sikkerhetskopi og gjenoppretting
- Sikkerhetsoppdateringer
- Lokalisering av IKT infrastruktur
- Beskyttelse av IKT infrastruktur
- Rutiner for sletting av data

Organisatoriske tiltak

- Internkontroller og bruk av sikkerhetsstandarder, slik om ISO 27.000-serien.
- Databehandlingsprotokoller
- Avviksbehandling
- Tredjepartskontroll

Personopplysninger knyttet til brukerprofil og til den som registrerer data blir lagret i databaser ved NGU, men er ikke tilgjengelige eksternt. Unntaket fra dette er i løsningene for oversikt over leveranser, der alle som har levert data kan se hvem som har registrert data innen samme bedrift (navn og eventuelt e-post). Personopplysninger som kan finnes i innmeldte dokumenter (som regel i pdf-format) er offentlig tilgjengelige gjennom kartinnsyn og nedlastingstjenester.

Databehandler har laget ROS analyse for behandling av personopplysninger i forbindelse med NADAG. Denne vil inneholde en kort oppsummering, inkludert risikovurdering, for hvilke personopplysninger som registreres, systemer/ databaser hvor informasjonen lagres. ROS-analysen kan oversendes på forespørsel.