Forskningsrådet

Introduksjon:

Dette er Norges Forskningsråd sin mal for databehandleravtaler på Norsk Bokmål, tilpasset for de tilfellene der Norges Forskningsråd opptrer som behandlingsansvarlig.

Malens felter merket parentes og/eller gul farge må slik det passer enten leses/forstås/fjernes, eller fylles ut for det konkrete tilfellet hver gang malen benyttes. De delene som er markert som alternative må velges og tilpasses tilsvarende.

Øvrig avtaletekst i malen bør også gjennomgås hver gang malen benyttes for å sikre at avtalen som inngås er tilpasset det konkrete formålet og den konkrete bruken i hvert enkelt tilfelle.

Malens avtaletekst begynner på dette dokumentets side 2.

Forskningsrådet

Databehandleravtale

I henhold til gjeldende norsk personopplysningslovgivning og forordning (EU) 2016/679 av 27. april 2016, Artikkel 28 og 29, jf. Artikkel 32-36, inngås følgende avtale

mellom

Norges forskningsråd, Org. nr. 970141669

(behandlingsansvarlig)

og

Sett inn navn på virksomhet, Org. nr. Sett inn Org. nr.

(databehandler)

Forskningsrådet

Begrep som benyttes i avtalen følger enten naturlig språklig forståelse, defineres i avtalen, eller leses slik de er definert i forordning (EU) 2016/679 av 27. april 2016, Artikkel 4.

1. Avtalens hensikt

Partene til denne Databehandleravtalen har inngått en avtale av (dato) («**Avtalen**») på bakgrunn av (bakgrunn/tema for hovedavtalen). Denne Databehandleravtalen regulerer partenes rettigheter og forpliktelser for å sikre at all Behandling av Personopplysninger skjer i henhold til gjeldende lovgivning om behandling av personopplysninger, herunder EUs personvernforordning 2016/679 («GDPR» og i gjeldende personvernlovgivning som gjennomfører denne.

Databehandleravtalen skal sikre at personopplysninger ikke brukes ulovlig, urettmessig eller at opplysningene behandles på måter som fører til uautorisert tilgang, endring, sletting, skade, tap eller utilgjengelighet.

Databehandleravtalen regulerer databehandlers forvaltning av personopplysninger på vegne av den behandlingsansvarlige, herunder innsamling, registrering, sammenstilling, lagring, prosessering, utlevering og sletting eller kombinasjoner av disse, i forbindelse med bruk av/behandling i (sett inn navn på tjeneste/prosjekt) (heretter omtalt som "tjenesten").

Ved motstrid skal vilkårene i denne avtalen gå foran databehandlers personvernerklæring eller vilkår i andre avtaler inngått mellom behandlingsansvarlig og databehandler i forbindelse med bruk av/behandling i tjenesten.

2. Behandlingens formål

Formålet med databehandlers forvaltning av personopplysninger på vegne av behandlingsansvarlig, er (sett inn en kort og presis beskrivelse av tjeneste/prosjekt og dets formål).

Personopplysninger som databehandler forvalter på vegne av behandlingsansvarlig kan ikke brukes til andre formål uten at dette på forhånd er godkjent av behandlingsansvarlig.

Databehandler kan ikke overføre personopplysninger som omfattes av denne avtalen til samarbeidspartnere eller andre tredjeparter uten at dette på forhånd er godkjent av behandlingsansvarlig, jf. punkt 10 i denne avtalen.

3. Instrukser

Behandlingsansvarlig har, som ansvarlig for at personopplysningene blir behandlet i samsvar med personvernlovgivningen, rett og plikt til å bestemme hvilke formål som skal gjelde og hvilke hjelpemidler som skal benyttes i behandlingen.

Behandlingsansvarlige skal gi databehandleren dokumenterte instrukser for hvordan personopplysninger skal behandles. Dersom ingen andre instrukser blir gitt, utgjør denne databehandleravtalen de gjeldende instruksene.

Databehandler skal bare behandle personopplysninger etter skriftlig instruks fra behandlingsansvarlig og skal følge de dokumenterte instruksene for forvaltning av personopplysninger i tjenesten som behandlingsansvarlig har bestemt skal gjelde.

Databehandler skal protokollføre alle behandlingsaktiviteter og overholde alle plikter i henhold til gjeldende norsk personopplysningslovgivning som gjelder ved bruk av tjenesten til behandling av personopplysninger.

Databehandler forplikter seg til å varsle behandlingsansvarlig dersom databehandler mottar instrukser fra behandlingsansvarlig som databehandleren mener er i strid med bestemmelsene i gjeldende norsk personopplysningslovgivning.

Databehandler skal på forespørsel bistå behandlingsansvarlig med å utføre en personvernkonsekvensvurdering, også kjent som en Data Protection Impact Assessment. Databehandler skal på samme måte etter anmodning bistå med å sikre at krav til innebygd personvern i databehandlers løsninger innfris. Dette inkluderer å bygge inn funksjonalitet for å oppfylle personvernprinsipper samt funksjonalitet for å sikre den registrertes rettigheter, så langt det med rimelighet kan forventes med hensyn til formålet med løsningen.

Kommentar: Detaljerte instrukser til databehandler kan legges ved som bilag til databehandleravtalen. Slike instrukser kan for eksempel innebære spesielle sikringstiltak, spesielle regler om sletting på gitte tidspunkter eller lignende.

4. Registrerte og opplysningstyper

Databehandler vil behandle personopplysninger i den utstrekning det er nødvendig for å oppfylle Avtalen. Kategorier av personopplysninger og kategorier av registrerte personer er spesifisert i **Bilag 1.**

5. De registrertes rettigheter

Databehandler plikter å bistå behandlingsansvarlig ved ivaretakelse av den registrertes rettigheter i henhold til gjeldende norsk personopplysningslovgivning.

Den registrertes rettigheter inkluderer retten til informasjon om hvordan hans eller hennes personopplysninger behandles, retten til å kreve innsyn i egne personopplysninger, retten til å kreve retting eller sletting av egne personopplysninger og retten til å kreve at behandlingen av egne personopplysninger begrenses.

I den grad det er relevant, skal databehandler bistå behandlingsansvarlig med å ivareta de registrertes rett til dataportabilitet og retten til å motsette seg automatiske avgjørelser, inkludert profilering.

6. Tilfredsstillende informasjonssikkerhet

Databehandler skal iverksette tilfredsstillende tekniske, fysiske og organisatoriske sikringstiltak for å beskytte personopplysninger som omfattes av denne avtalen mot uautorisert eller ulovlig tilgang, endring, sletting, skade, tap eller utilgjengelighet.

Databehandler skal dokumentere egen sikkerhetsorganisering, retningslinjer og rutiner for sikkerhetsarbeidet, risikovurderinger og etablerte tekniske, fysiske eller organisatoriske

sikringstiltak. Dokumentasjonen skal være tilgjengelig for behandlingsansvarlig på forespørsel.

Databehandler skal etablere kontinuitets- og beredskapsplaner for effektiv håndtering av alvorlige sikkerhetshendelser. Dokumentasjonen skal være tilgjengelig for behandlingsansvarlig på forespørsel.

Databehandler skal gi egne ansatte tilstrekkelig informasjon om og opplæring i informasjonssikkerhet slik at sikkerheten til personopplysninger som behandles på vegne av behandlingsansvarlig blir ivaretatt.

En detaljert beskrivelse av tiltak for informasjonssikkerhet vedlegges i **Bilag 2.**

Kommentar: Her er det behov for å konkretisere de viktigste sikringstiltakene som databehandleren har iverksatt, eventuelt at det henvises til dokumenter eller publikasjoner som forklarer hvordan databehandleren jobber med informasjonssikkerhet og hvilke sikringstiltak som er etablert for den aktuelle tjenesten. Konkretiseringene tas i bilag 2 til avtalen.

7. Taushetsplikt

Kun ansatte hos databehandler som har tjenstlige behov for tilgang til personopplysninger som forvaltes på vegne av behandlingsansvarlig, kan gis slik tilgang. Databehandler plikter å dokumentere retningslinjer og rutiner for tilgangsstyring. Dokumentasjonen skal være tilgjengelig for behandlingsansvarlig på forespørsel.

Databehandler og de ansatte hos databehandler har konfidensialitets- og taushetsplikt om dokumentasjon og personopplysninger som vedkommende får tilgang til i henhold til denne avtalen. Konfidensialitets- og taushetsplikten omfatter tredjeparter og deres ansatte som utfører oppdrag som underdatabehandler eller utfører vedlikehold (eller liknende oppgaver) av systemer, utstyr, nettverk eller bygninger som databehandler anvender for å levere tjenesten. Konfidensialitets- og taushetspliktene gjelder også etter Avtalens opphør.

Databehandler plikter å dokumentere at de som her er pålagt taushetsplikt har mottatt informasjon om taushetsplikten og samtykket til å være bundet av denne. Dokumentasjonen skal være tilgjengelig for behandlingsansvarlig på forespørsel.

Norsk lov vil kunne begrense omfanget av taushetsplikten for ansatte hos databehandler og tredjeparter.

8. Tilgang til informasjon og sikkerhetsdokumentasjon

Behandlingsansvarlig har, med mindre annet er avtalt eller følger av lov, rett til tilgang til og innsyn i personopplysningene som databehandleren håndterer og de systemene som benyttes til dette formål. Databehandler skal på forespørsel gjøre tilgjengelig for behandlingsansvarlig de behandlede personopplysningene og all informasjon om behandlingen som er nødvendig for å påvise om partenes forpliktelser er oppfylt eller ikke. Databehandler plikter å gi nødvendig bistand i denne forbindelse.

Databehandler plikter på forespørsel å gi behandlingsansvarlig tilgang til all sikkerhetsdokumentasjon som er nødvendig for at behandlingsansvarlig skal kunne ivareta sine forpliktelser i henhold til gjeldende norsk personopplysningslovgivning, samt å samarbeide med behandlingsansvarlig og tilsynsmyndigheten i denne forbindelse.

Behandlingsansvarlig har taushetsplikt for konfidensiell sikkerhetsdokumentasjon som databehandler gjør tilgjengelig for behandlingsansvarlig.

9. Varslingsplikt ved sikkerhetsbrudd

Databehandler skal uten ugrunnet opphold varsle behandlingsansvarlig dersom personopplysninger som forvaltes på vegne av behandlingsansvarlig utsettes for sikkerhetsbrudd.

Varselet til behandlingsansvarlig skal som minimum inneholde informasjon som beskriver sikkerhetsbruddet, hvilke registrerte som er berørt av sikkerhetsbruddet, hvilke personopplysninger som er berørt av sikkerhetsbruddet, hvilke strakstiltak som er iverksatt for å håndtere sikkerhetsbruddet og hvilke forebyggende tiltak som eventuelt er etablert for å unngå liknende hendelser i fremtiden.

Behandlingsansvarlig er ansvarlig for at Datatilsynet blir varslet når dette er påkrevd.

10. Underleverandører

Databehandler plikter før behandlingen av personopplysninger starter å inngå egne avtaler med underleverandører som regulerer underleverandørenes forvaltning av personopplysninger i forbindelse med denne avtalen.

I avtaler mellom databehandler og underleverandører skal underleverandørene pålegges å ivareta alle plikter som databehandleren selv er underlagt i henhold til denne avtalen og lovverket. Databehandler plikter å forelegge avtalene for behandlingsansvarlig på forespørsel.

Databehandler skal kontrollere at underleverandører overholder sine avtalemessige plikter, spesielt at informasjonssikkerheten er tilfredsstillende og at ansatte hos underleverandører er kjent med sine forpliktelser og oppfyller disse.

Behandlingsansvarlig godkjenner at databehandler engasjerer følgende underleverandører for å oppfylle denne avtalen: se **Bilag 3.**

Databehandler kan ikke engasjere andre underleverandører enn de som er nevnt ovenfor uten at dette på forhånd er skriftlig godkjent av behandlingsansvarlig.

Databehandler er ansvarlig for underleverandørens handlinger og unnlatelser som om de var databehandlerens egne.

I tilfeller der den behandlingsansvarlige har godkjent bruk av en underleverandør i henhold til **Bilag 3,** skal databehandleren påse at underleverandøren etterlever eventuelle krav til undertegning av EUs standardavtale og tilleggstiltak i henhold til denne databehandleravtalens punkt 12.

Databehandler plikter å ikke ta i bruk underleverandører før vilkårene i dette punkt 10 og punkt 12 er oppfylt.

11. Behandlingsplaner

Både Databehandler og underleverandører av Databehandler plikter å utarbeide og følge eget prosedyreverk/behandlingsplan som sikrer at deres behandling av personopplysninger utføres i henhold til deres respektive inngåtte databehandleravtale.

Slikt prosedyreverk/behandlingsplan skal fremlegges for Behandlingsansvarlig for dennes kvalitetssikring og godkjenning før behandlingen kan iverksettes.

12. Overføring til land utenfor EU/EØS

Kommentar: Personopplysninger som databehandler forvalter på vegne av behandlingsansvarlig kan i noen tilfeller, og da avhengig av at Norges Forskningsråds retningslinjer og øvrig lovverk slik som f. eks Arkivloven åpner for det, bli tillatt overført til land utenfor Norden og/eller EU. Slik overføring kan skje på visse vilkår og regler om overføring til tredjestater som blant annet finnes i Artikkel 45-47 og 49 i EUs personvernforordning, i tillegg til kravene fastsatt av EU-domstolen i Schrems II-dommen. Reglene gjelder også for sikkerhetskopiering og annen overføring av personopplysninger som skjer i forbindelse med administrasjon av den aktuelle tjenesten, for eksempel support.

Innenfor EU/EØS

Personopplysninger som databehandler forvalter i henhold til denne avtalen, vil bli overført til følgende mottakerland innenfor EU/EØS: **Se bilag 3**

Utenfor EU/EØS

For å overholde kravene i personopplysningslovgivningen for overføring av personopplysninger til databehandler/underleverandører hvor behandlingen utføres utenfor EU/EØS, skal databehandler sørge for at det ikke overføres personopplysninger til land utenfor EØS-området uten overføringsgrunnlag i henhold til personopplysningslovgivningen og dokumentasjon som påviser at vilkårene for å benytte overføringsgrunnlaget er oppfylt.

Overføringer må også oppfylle tilleggskravene fastsatt av EU-domstolen i (EU) C-311/18 (**Schrems II-dommen**). Databehandleren skal i et slikt tilfelle dokumentere dette i **bilag 3**. Identifisering og implementering av tilleggstiltak skal skje for databehandlerens regning.

Databehandler skal også gi nødvendig dokumentasjon om sikkerhet, samsvar og risiko knyttet til aktuelt selskap og plassering. Basert på tilgjengelig dokumentasjon og beskrivelser skal databehandler og behandlingsansvarlig i samarbeid utarbeide en særskilt risikovurdering som skal brukes som beslutningsgrunnlag.

Personopplysninger som databehandler forvalter i henhold til denne avtalen, vil bli overført til følgende mottakerland utenfor EU/EØS: **se bilag 3.**

Det rettslige grunnlaget for overføring av personopplysninger til de nevnte mottakerland utenfor EU/EØS er: **se bilag 3.**

13. Sikkerhetsrevisjoner og konsekvensutredninger

Databehandler skal jevnlig gjennomføre sikkerhetsrevisjoner av eget arbeid med sikring av personopplysninger mot uautorisert eller ulovlig tilgang, endring, sletting, skade, tap eller utilgjengelighet.

Sikkerhetsrevisjoner skal omfatte databehandlers sikkerhetsmål og sikkerhetsstrategi, sikkerhetsorganisering, retningslinjer og rutiner for sikkerhetsarbeidet, etablerte tekniske, fysiske og organisatoriske sikringstiltak og arbeidet med informasjonssikkerhet hos underleverandører til denne avtalen. Det skal i tillegg omfatte rutiner for varsling av behandlingsansvarlig ved sikkerhetsbrudd og rutiner for testing av beredskaps- og kontinuitetsplaner.

Databehandler skal dokumentere sikkerhetsrevisjonene. Behandlingsansvarlig skal gis tilgang til revisjonsrapportene på forespørsel.

Dersom en uavhengig tredjepart gjennomfører sikkerhetsrevisjoner hos databehandler, skal behandlingsansvarlig informeres om hvilken revisor som benyttes og få tilgang til oppsummeringer av revisjonsrapportene på forespørsel.

Kommentar: Partene kan hvis ønskelig avtale at behandlingsansvarlig selv, eller en uavhengig tredjepart som behandlingsansvarlig selv velger, utfører sikkerhetsrevisjoner hos databehandleren, og eventuelt hvordan kostnader som påløper i forbindelse med slike revisjoner skal fordeles.

14. Tilbakelevering og sletting

Ved opphør av denne avtalen plikter databehandler å tilbakelevere og slette alle personopplysninger som forvaltes på vegne av behandlingsansvarlig i henhold til denne avtalen. Behandlingsansvarlig bestemmer hvordan tilbakelevering av personopplysningene skal skje, herunder hvilket format som skal benyttes.

Sletting skal skje ved at databehandler sletter personopplysninger innen (sett inn antall) dager etter avtalens opphør, med mindre preseptorisk lovgivning forhindrer Databehandler fra slik sletting. Dette gjelder også for sikkerhetskopier av personopplysningene.

Databehandler skal dokumentere og kunne bekrefte at sletting av personopplysninger er foretatt i henhold til denne avtalen. Dokumentasjonen og bekreftelsen skal gjøres tilgjengelig for behandlingsansvarlig på forespørsel.

Databehandler dekker alle kostnader i forbindelse med tilbakelevering og sletting av de personopplysninger som omfattes av denne avtalen.

15. Mislighold

Ved mislighold av vilkårene i denne databehandleravtalen som skyldes feil eller forsømmelser fra databehandlers side, kan behandlingsansvarlig si opp avtalen med øyeblikkelig virkning. Slikt mislighold vil utgjøre et vesentlig mislighold av Avtalen. Databehandler vil fortsatt være pliktig til å tilbakelevere og slette personopplysninger som forvaltes på vegne av behandlingsansvarlig i henhold til bestemmelsene i punkt 14 ovenfor.

Se Avtalens punkt XX (sett inn punktnummeret på erstatsningsbestemmelsen som du finner i Avtalen (anskaffelsesavtalen)) for reguleringen av erstatningsansvar. I den grad databehandlerens underleverandører bryter noen av forpliktelsene iht. denne databehandleravtalen er Databehandler på samme måte erstatningsansvarlig ovenfor Behandlingsansvarlig.

Forskningsrådet

16. Avtalens varighet

Denne databehandleravtalen gjelder frem til opphør av Avtalen.

17. Kontaktpersoner

Kontaktperson hos databehandler for spørsmål knyttet til denne avtalen er: (sett inn navn og kontaktinformasjon til kontaktperson hos databehandler).

Kontaktperson hos behandlingsansvarlig for spørsmål knyttet til denne avtalen er: (sett inn navn og kontaktinformasjon til kontaktperson hos behandlingsansvarlig).

Brudd på personopplysningssikkerheten skal meldes til behandlingsansvarliges personvernombud på e-post: "personvern@forskningsradet.no" eller telefon: +47 22 03 70 00

Kommentar: Stryk det alternativet nedenfor (18a eller b) som ikke passer

18a. Lovvalg og verneting

Avtalen er underlagt norsk rett og partene vedtar Oslo som verneting. Dette gjelder også etter opphør av avtalen.

Kommentar: Dette punktet benyttes når databehandler er en privat aktør.

18b. Lovvalg og tvisteløsning

Partenes rettigheter og plikter etter denne avtalen bestemmes i sin helhet av norsk rett. Eventuelle tvister som springer ut av denne avtalen skal først søkes løst gjennom forhandlinger.

Dersom partene ikke oppnår enighet gjennom forhandlinger, skal tvisten løses med bindende virkning av Kunnskapsdepartementet. Hver av partene kan forlange at tvisten oversendes departementet.
Kommentar: Dette punktet benyttes når databehandler er en Norsk statlig aktør.

***

Denne avtale er i 2 – to eksemplarer, hvorav partene beholder hvert sitt.

(Sett inn sted og dato)

Forskningsrådet

På vegne av behandlingsansvarlig	På vegne av databehandler
Navn: (sett inn navn)	Navn: (sett inn navn)
Stilling: (sett inn stilling)	Stilling: (sett inn stilling)
……..	……
(underskrift)	(underskrift)

Forskningsrådet

BILAG 1 REGISTRERTE OG KATEGORIER AV OPPLYSNINGER

Registrerte

- Sett inn en kort og presis oversikt over hvilke typer registrerte opplysningene gjelder. Eksempler er: ansatte, innleide, brukere, deltakere, besøkende, nettstedsbesøkende, leverandører, andre tredjeparter eller lignende.

Kategorier opplysninger

- Sett inn en kort og presis oversikt (gjerne punktvis) over hvilke kategorier personopplysninger som databehandler forvalter på vegne av behandlingsansvarlig. Eksempler er: navn, telefonnummer, adresse, e-postadresse, fødsels- og personnummer, stilling/rolle, organisasjon, ansettelsesforhold, samtaler eller annen kommunikasjon, respons på markedsføring, analyser og rapporter om registrerte, personlige finansielle transaksjoner, handel.

Særlige kategorier opplysninger

- Sett inn en kort og presis oversikt (gjerne punktvis) over hvilke særlige kategorier personopplysninger som databehandler forvalter på vegne av behandlingsansvarlig. Eksempler er sensitive opplysninger slik som: helseopplysninger, etnisitet, politisk/religiøs/filosofisk/seksuell preferanse, fagforeningstilhørighet, genetiske data med det formål entydig å identifisere en fysisk person, biometriske data med det formål entydig å identifisere en fysisk person.

Ytterligere opplysninger

Sett inn en kort og presis oversikt (gjerne punktvis) over hvilke ytterligere opplysninger som databehandler registrerer og lagrer i forbindelse med bruk av tjenesten. Eksempler er: bruk av informasjonskapsler, sikkerhetskopier, merke og modell, IP-adresse, MAC-adresse, serienummer, posisjonsdata, start- og slutt-tid for kommunikasjon, størrelsen på melding, kontekst, adgangskontroll logger (fysiske/logiske), CCTV-opptak, lydopptak, kjøreovervåkningsdata, eller andre typer data og metadata.

Forskningsrådet

BILAG 2 INFORMASJONSSIKKERHET

Kommentar: Her er det være behov for å konkretisere de viktigste sikringstiltakene som databehandleren har iverksatt, eventuelt at det henvises til dokumenter eller publikasjoner som forklarer hvordan databehandleren jobber med informasjonssikkerhet og hvilke sikringstiltak som er etablert for den aktuelle tjenesten.

Forskningsrådet

BILAG 3 BRUK AV UNDERLEVERANDØRER (UNDERDATABEHANDLERE) OG OVERFØRING TIL LAND

1. **Overføring til databehandler, land:**

Kommentar:

-Sett inn informasjon om databehandlers/leverandørens geografiske plassering.

2. **Overføring til underleverandører (underdatabehandler), navn og land:**

Kommentar:

-Sett inn informasjon om underdatabehandlere/underleverandørene:

Navn	Behandlingsaktivitet	Sted

3. **Overføringsgrunnlag:**

Databehandler/underleverandør skal ikke overføre personopplysninger ut av EØS, eller gi underleverandører utenfor EØS tilgang til personopplysninger, uten etter skriftlig samtykke fra behandlingsansvarlig.

Ved samtykke til overføring av personopplysninger til et land utenfor EØS-området, som ikke er ansett å sikre forsvarlig behandling i henhold til GDPR Artikkel 45, plikter databehandler å inngå avtale på grunnlag av EUs standardavtaler for overføring til databehandlere i tredjeland ((EU) 2021/914) eller annen slik standardavtale som eventuelt har avløst denne.

I disse tilfellene skal databehandler forplikte seg til å påse at tilgang til eller behandling av personopplysninger ikke skjer før:

(i) EUs standardavtaler er undertegnet av den EØS-baserte databehandleren som data eksportør og den ikke EØS-baserte databehandler eller underleverandør som data importør, og

(ii) Databehandler har mottatt den behandlingsansvarliges utvetydige bekreftelse på at eventuelle krav om å gi melding eller innhente godkjenning fra datatilsynsmyndighetene før overføringen anses å være ivaretatt.

Forskningsrådet

Kommentar:

-Dersom databehandling skal skje utenfor EU/EØS (eller land som er godkjent av EU som land som har et tilfredsstillende regelverk for behandling av personopplysninger, se liste her) må det sikres at slik behandling er underlagt tilsvarende strenge regler som personopplysningsloven/GDPR.

Obs! Tilsvarende gjelder for eventuelle underdatabehandlere til databehandleren. Altså må man sikre at underdatabehandleren også er underlagt tilsvarende strenge regler dersom denne befinner seg i et tredjeland.

Det skal det ikke overføres personopplysninger til land utenfor EØS-området uten overføringsgrunnlag og dokumentasjon som påviser at vilkårene for å benytte overføringsgrunnlaget er oppfylt.