

AVTALE OM Arbeidsrettet rehabilitering

Databehandleravtale

mellom

Arbeids- og velferdsetaten (NAV)
som Behandlingsansvarlig

og

[Virksomhetens navn]
som Databehandler

Sted og dato:

For Behandlingsansvarlig (NAV)

For Databehandler

Inger Anderssen

Behandlingsansvarlig (NAV)

Virksomheten

Avtalen signeres digitalt i Mercell

INNHALDSFORTEGNELSE:

1	Formålet med denne databehandleravtalen	3
2	Definisjoner	3
3	Omfang av behandlingen.....	4
4	Generelle plikter	5
5	Bistand til behandlingsansvarlig.....	5
6	Tekniske og organisatoriske sikkerhetstiltak	6
7	Taushetsplikt.....	6
8	Bruk av underdatabehandlere	7
9	Overføring av personopplysninger til tredjeland.....	7
10	Melding om brudd på personopplysningssikkerheten.....	8
11	Revisjon	8
12	Varighet og opphør	9
13	Lovvalg og verneting.....	9
14	Kontaktpersoner.....	10
15	Vedlegg 1 Databehandlingens omfang	10
16	Vedlegg 2 Tekniske og organisatoriske sikkerhetstiltak	12
17	Vedlegg 3 Godkjente underdatabehandlere	14

1 FORMÅLET MED DENNE DATABEHANDLERAVTALEN

1. Denne avtalen ("Databehandleravtalen") er en del av Arbeidsrettet rehabiliterings tiltaket ("Hovedavtalen") datert [dato] mellom NAV Tiltak Agder («Behandlingsansvarlig») og [navn] ("Databehandler"), der begge utgjør en "Part", samlet benevnt som "Partene".
2. Databehandleravtalens hensikt er å regulere rettigheter og plikter i henhold til Europaparlamentets- og rådsforordning (EU) 2016 av 27. april 2016 og lov om behandling av personopplysninger (LOV-2018-06-15-38).
3. Databehandleravtalen regulerer Databehandlers Behandling av Personopplysninger på vegne av Behandlingsansvarlig i forbindelse med Hovedavtalen.
4. I tilfelle uoverensstemmelse mellom Hovedavtalen og Databehandleravtalen når det gjelder forhold spesifikt knyttet til personvern, skal Databehandleravtalen gis forrang.
5. Ved motstrid mellom Databehandleravtalen og andre avtaler mellom Partene, har Databehandleravtalen forrang når det gjelder forhold spesifikt knyttet til taushetsplikt og behandling av personopplysninger. Ved motstrid mellom Databehandleravtalen og eventuelt inngått Standard Contractual Clauses (SCC), har SCC forrang.
6. Databehandleravtalen har tre vedlegg. Vedleggene er en del av Databehandleravtalen. I tilfelle uoverensstemmelse mellom Databehandleravtalen og vedleggene, skal vedleggene gis forrang.
7. Vedlegg 1 inneholder en beskrivelse av Behandlingens omfang, formål, art, type Personopplysninger, kategorier av registrerte og varighet av Behandlingen.
8. Vedlegg 2 inneholder en beskrivelse av tekniske og organisatoriske sikkerhetstiltak.
9. Vedlegg 3 inneholder en oversikt over godkjente Underdatabehandlere.

2 DEFINISJONER

I Databehandleravtalen skal følgende ord og uttrykk ha tilsvarende betydning som etter GDPR:

1. «**Personopplysninger**»: Enhver opplysning om en identifisert eller identifiserbar fysisk person («den registrerte»). En identifiserbar fysisk person er en person som direkte eller indirekte kan identifiseres, særlig ved hjelp av en eller flere identifikatorer. Slike identifikatorer kan f.eks. være et navn, et identifikasjonsnummer, lokaliseringsopplysninger, en online-identifikator eller ett eller flere elementer som er spesifikke for nevnte fysiske persons fysiske, fysiologiske, genetiske, psykiske, økonomiske, kulturelle eller sosiale identitet, se artikkel 4 nr. 1.
2. «**Behandling**»: Enhver operasjon eller rekke av operasjoner som gjøres med personopplysninger, enten automatisert eller ikke, f.eks. innsamling, registrering, organisering, strukturering, lagring, tilpasning eller endring, gjenfinning, konsultering, bruk, utlevering ved overføring, spredning eller alle andre former for tilgjengeliggjøring, sammenstilling eller samkjøring, begrensning, sletting eller tilintetgjøring. Det omfatter

også tilgang til å se på personopplysningene, aksessere, samt aksessering fra annen lokasjon (fjernaksess), og eller mulighet til å aksessere personopplysninger, selv om denne muligheten ikke faktisk benyttes, både fra fjern og nær lokasjon. Se artikkel 4 nr. 2.

3. «**Behandlingsansvarlig**»: en fysisk eller juridisk person, en offentlig myndighet, en institusjon eller ethvert annet organ som alene eller sammen med andre bestemmer formålet med behandlingen av personopplysninger og hvilke midler som skal benyttes; når formålet med og midlene for behandlingen er fastsatt i unionsretten eller i medlemsstatenes nasjonale rett, kan den behandlingsansvarlige, eller de særlige kriteriene for utpeking av vedkommende, fastsettes i unionsretten eller i medlemsstatenes nasjonale rett.
4. «**Databehandler**»: en fysisk eller juridisk person, offentlig myndighet, institusjon eller ethvert annet organ som behandler personopplysninger på vegne av den behandlingsansvarlige.
5. «**Brudd på personopplysningssikkerheten**»: Brudd på sikkerheten som fører til utilsiktet eller ulovlig tilintetgjøring, tap, endring, ulovlig spredning av eller tilgang til personopplysninger som er overført, lagret eller på annen måte behandlet, se artikkel 4 nr. 12.
6. «**Underdatabehandler**»: En annen databehandler eller flere (underleverandører) som Databehandler engasjerer for å utføre spesifikke Behandlinger på vegne av Behandlingsansvarlig.
7. «**GDPR**»: General Data Protection Regulation. Europaparlamentets- og rådsforordning (EU) 2016/679 av 27. april 2016 om vern av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger samt om oppheving av direktiv 95/46/EF (generell personvernforordning).
8. «**Gjeldende personvernregler**»: Til enhver tid gjeldende lover og regler om personvern, inkludert personopplysningsloven og GDPR.
9. «**Tredjestat**»: Et land utenfor EØS.

For øvrig skal ord og uttrykk ha samme mening som de er tillagt i GDPR.

3 OMFANG AV BEHANDLINGEN

1. Databehandleravtalen gjelder alle Personopplysninger som Databehandler skal behandle på vegne av Behandlingsansvarlig, f.eks. Personopplysninger som Databehandler har mottatt, er gitt tilgang til eller har generert i forbindelse med Hovedavtalen.
2. Behandlingens omfang, formål, art, type Personopplysninger, kategorier av registrerte og varighet av Behandlingen fremgår av Vedlegg 1.
3. Databehandler har ikke selvstendig råderett over Personopplysningene og kan ikke bruke opplysningene til andre formål enn det som fremgår av Vedlegg 1, med mindre det kreves i henhold til unionsretten eller medlemsstatenes nasjonale rett som Databehandleren er

underlagt. I så fall skal Databehandleren underrette den Behandlingsansvarlige om nevnte rettslige krav før Behandlingen, men mindre denne rett av hensyn til viktige allmenne interesser forbyr en slik underretning Databehandleren skal ellers behandle Personopplysningene i samsvar med Behandlingsansvarliges dokumenterte instruksjer.

4 GENERELLE PLIKTER

1. Databehandler plikter å utføre Behandlingen av Personopplysningene i samsvar med krav som stilles til databehandlere etter Gjeldende personvernregler.
2. Databehandler skal omgående varsle Behandlingsansvarlig skriftlig hvis Databehandler har rimelig grunn til å tro at:
 - (i) en instruks fra Behandlingsansvarlig kan medføre at Databehandler bryter med Gjeldende personvernregler, eller
 - (ii) gjeldende rett i EØS-området krever at Databehandler behandler Personopplysninger utover omfanget av Behandlingsansvarliges dokumenterte instruksjer.

I tilfelle av (i) eller (ii) skal Partene diskutere hvordan problemet kan løses uten at de registrertes rettigheter blir krenket.

3. Databehandler skal umiddelbart varsle Behandlingsansvarlig hvis den mottar forespørsel fra en myndighet om å utlevere Personopplysninger som er behandlet under Databehandleravtalen. Med mindre loven krever det, skal Databehandler ikke etterkomme en slik forespørsel uten skriftlig forhåndsgodkjenning fra Behandlingsansvarlig.
4. Hvis Databehandler er underlagt godkjente atferdsnormer etter GDPR artikkel 40 eller en godkjent sertifiseringsmekanisme etter GDPR artikkel 42, garanterer Databehandler at den vil etterleve slike atferdsnormer eller sertifiseringsmekanismer.
5. Dersom Databehandler er underlagt plikt om protokollføring som fremgår av GDPR artikkel 30 skal Databehandler føre skriftlig protokoll over alle kategorier av Behandlinger som utøves på vegne av Behandlingsansvarlig.

5 BISTAND TIL BEHANDLINGSANSVARLIG

1. Databehandler plikter å bistå Behandlingsansvarlig ved oppfyllelse av registrertes rettigheter etter GDPR kapittel III.
2. Databehandleren skal bistå Behandlingsansvarlig med forpliktelsene etter GDPR artikkel 32 til 36, herunder Behandlingsansvarliges forpliktelser til å gjennomføre tekniske og organisatoriske sikkerhetstiltak, å gi melding til registrerte og Datatilsynet om Brudd på personopplysningssikkerhet, vurdering av personvernkonsekvenser samt forhåndsdrøftinger med Datatilsynet.

3. Ved behov for bistand som nevnt i dette punkt 5 skal Behandlingsansvarlig sende en skriftlig henvendelse til Databehandler.
4. Databehandler skal umiddelbart videresende til Behandlingsansvarlig forespørsler eller klager som Databehandler eventuelt mottar fra den registrerte.

6 TEKNISKE OG ORGANISATORISKE SIKKERHETSTILTAK

1. Databehandler skal gjennomføre egnede tekniske, fysiske og organisatoriske sikkerhetstiltak for å beskytte Personopplysninger som omfattes av Databehandleravtalen mot utilsiktet eller ulovlig tilintetgjøring, tap, endring og ikke-autorisert utlevering eller tilgang. Databehandleren skal som et minimum gjennomføre de tiltakene som er påkrevd i henhold til GDPR artikkel 32, samt de tiltak som er angitt eller referert til i Vedlegg 2.
2. I henhold til GDPR artikkel 32 skal Databehandleren – uavhengig av Behandlingsansvarlig – også vurdere risikoene som Behandlingen utgjør for fysiske personers rettigheter og gjennomføre tiltak for å imøtegå disse risikoene. I forbindelse med denne vurderingen, skal Behandlingsansvarlig stille nødvendig informasjon til rådighet for Databehandleren som gjør vedkommende i stand til at identifisere og vurdere risikoene.
3. Databehandler skal ikke utlevere Personopplysninger til tredjeparter uten skriftlig forhåndsgodkjenning fra Behandlingsansvarlig. Unntak gjelder for overføring til eventuelle godkjente Underdatabehandlere (se avtalens punkt 8) når de har behov for Personopplysningene for å kunne utføre sine oppgaver.
4. Databehandler skal sikre at kun de personer som er autorisert til å behandle Personopplysninger, har tilgang til Personopplysningene som behandles på vegne av Behandlingsansvarlig.

7 TAUSHETSPLIKT

1. Databehandlers ansatte og andre som opptrer på Databehandlers vegne, har taushetsplikt om informasjon og Personopplysninger som vedkommende får tilgang til etter Databehandleravtalen. Taushetsplikten omfatter også ansatte hos Underdatabehandler som utfører oppdrag for Databehandler for å kunne levere tjenesten.
2. Ansatte og andre hos Databehandler pålegges taushetsplikt etter reglene i arbeids- og velferdsforvaltningsloven § 7, jf. forvaltningsloven §§ 13 til 13 e og 13 g. Taushetsplikten omfatter også opplysninger om fødested, fødselsdato, personnummer, statsborgerforhold, sivilstand, yrke, bosted og arbeidssted, jf. arbeids- og velferdsforvaltningsloven § 7, første ledd. NAVs taushetsplikterklæring skal undertegnes.
3. Taushetsplikten gjelder også etter Databehandleravtalens opphør. Ansatte og andre som fratrer sin tjeneste hos Databehandler skal pålegges taushet også etter fratredelse om forhold som nevnt ovenfor.

8 BRUK AV UNDERDATABEHANDLERE

1. Databehandler kan kun engasjere Underdatabehandlere etter forutgående skriftlig tillatelse fra Behandlingsansvarlig. Godkjente Underdatabehandlere er oppført i Vedlegg 3.
2. Databehandler skal kun engasjere Underdatabehandlere som gjennomfører egnede tekniske og organisatoriske tiltak som sikrer at Behandlingen oppfyller kravene etter Gjeldende personvernregler. Databehandler skal gjennomføre kontroller av Underdatabehandlere for å verifisere deres databeskyttelsesnivå. Databehandler skal kunne fremlegge rapporter fra slik kontroller for Behandlingsansvarlig.
3. Databehandler plikter å inngå skriftlig avtale med hver Underdatabehandler som regulerer Underdatabehandlers Behandling av Personopplysninger og pålegges å ivareta alle plikter med hensyn til vern av Personopplysninger som Databehandleren selv er underlagt etter denne Databehandleravtalen. Databehandler plikter å forelegge disse avtalene for Behandlingsansvarlig etter forespørsel.
4. Databehandleren skal i sin avtale med Underdatabehandleren innta Behandlingsansvarlig som begunstiget tredjeperson i tilfelle Databehandleren går konkurs, slik at Behandlingsansvarlig kan tre inn i Databehandlerens rettigheter og gjøre dem gjeldende over for Underdatabehandlere, som f.eks. gjør den Behandlingsansvarlige i stand til å instruere Underdatabehandleren i å slette eller tilbakelevere Personopplysningene.
5. Databehandler har fullt ansvar for Underdatabehandlers utførelse av sine forpliktelser på samme måte som om Databehandler selv sto for utførelsen.
6. Samtlige som på vegne av Databehandler utfører oppdrag der Behandling av de aktuelle Personopplysningene inngår, skal være kjent med Databehandlers avtalemessige og lovmessige forpliktelser og oppfylle disse.

9 OVERFØRING AV PERSONOPPLYSNINGER TIL TREDJESTAT

1. Databehandler kan kun overføre Personopplysninger til en Tredjestat eller en internasjonal organisasjon etter dokumenterte instruksjoner fra Behandlingsansvarlig. Databehandler skal i den forbindelse også dokumentere gyldig overføringsgrunnlag.
2. Unntak kan skje dersom det kreves i henhold til gjeldende rett i EØS-området. I slike tilfeller skal Databehandler underrette Behandlingsansvarlig om nevnte rettslige krav før overføringen, med mindre denne rett av hensyn til viktige samfunnsinteresser forbyr slik underretning (i så fall skal Databehandleren underrette Behandlingsansvarlig så snart dette er tillatt).

10 MELDING OM BRUDD PÅ PERSONOPPLYSNINGSSIKKERHETEN

1. Databehandler skal gi skriftlig melding til Behandlingsansvarlig om eventuelle Brudd på personopplysningssikkerheten, samt bistå Behandlingsansvarlig med det som er nødvendig for at Behandlingsansvarlig skal kunne gi melding om Brudd på personopplysningssikkerheten til Datatilsynet etter GDPR artikkel 33.
2. Melding til Behandlingsansvarlig om Brudd på personopplysningssikkerheten skal gis uten ugrunnet opphold og senest innen 24 timer etter at Databehandler ble oppmerksom på bruddet, slik at Behandlingsansvarlig har mulighet til å melde bruddet til Datatilsynet innenfor tidsfristen på 72 timer.
3. Melding til Behandlingsansvarlig om Brudd på personopplysningssikkerheten bør inneholde en beskrivelse av:
 - a. arten av bruddet, herunder kategoriene av og omtrentlig antall registrerte som er berørt, og kategoriene av og omtrentlig antall personopplysningsposter som er berørt,
 - b. de berørte registrertes identitet,
 - c. navn og kontaktinformasjon til Personvernombudet eller et annet kontaktpunkt hos Databehandler for ytterligere innhenting av informasjon,
 - d. de sannsynlige konsekvensene av Bruddet på personopplysningssikkerheten,
 - e. tiltak som er truffet eller foreslått for å håndtere Bruddet på personopplysningssikkerheten, herunder tiltak for å redusere eventuelle skadevirkninger,
 - f. annen informasjon som kreves for at Behandlingsansvarlig kan overholde Gjeldende personvernregler.

Informasjonen som nevnt i bokstav a-f skal gis uten ugrunnet opphold, men den kan gis trinnvis i den grad det er nødvendig.

Databehandler skal så snart som mulig gjennomføre alle tiltak som beskrevet i punkt e ovenfor. I tillegg skal Databehandler gjennomføre alle de tiltak som med rimelighet kreves for å unngå at det senere oppstår lignende Brudd på personopplysningssikkerheten. Databehandler skal, så langt det er mulig, rådføre seg med Behandlingsansvarlig om de tiltak som skal gjennomføres samt overveie innspill fra Behandlingsansvarlig i den forbindelse.

4. Kun Behandlingsansvarlig har rett til å rapportere til Datatilsynet og til de berørte registrerte om Brudd på personopplysningssikkerheten. Databehandler skal avstå fra å informere allmennheten eller tredjepart om Brudd på personopplysningssikkerheten.

11 REVISJON

1. Databehandler skal dokumentere og gjøre tilgjengelig for Behandlingsansvarlig, informasjon som er nødvendig for å påvise etterlevelse av Databehandleravtalen og Gjeldende personvernregler.
2. Databehandler skal muliggjøre og bidra ved revisjoner som utføres av Behandlingsansvarlig eller av en uavhengig tredjepart med fullmakt fra Behandlingsansvarlig. Databehandler skal også muliggjøre og bidra ved revisjoner fra tilsynsmyndigheter.

3. Databehandleren skal foreta jevnlig revisjoner av sine Behandlinger. Dette kan Databehandler gjøre på egen hånd eller via en uavhengig tredjepart med fullmakt fra Databehandler. Databehandleren skal oversende kopi av revisjonsrapporter fra slike revisjoner til Behandlingsansvarlig. Behandlingsansvarlig skal ha rett til å fremlegge slike revisjonsrapporter til sine eksterne revisorer og tilsynsmyndigheter.
4. Dersom en revisjon avdekker avvik fra forpliktelsene i Databehandleravtalen, skal Databehandler så snart som mulig avhjelpe slike avvik (og, hvis relevant, påse at den relevante underdatabehandler gjør det samme). Behandlingsansvarlig kan kreve at hele eller deler av behandlingsaktivitetene midlertidig opphører til vellykket utbedring er bekreftet. Ved særlig alvorlige brudd kan Behandlingsansvarlig kreve at Behandlingen stoppes, Personopplysningene tilbakeføres til Behandlingsansvarlig og at Hovedavtalen samt Databehandleravtalen termineres.
5. Hver av partene dekker sine egne kostnader forbundet med en revisjon. Hvis en revisjon avdekker avvik fra forpliktelsene i Databehandleravtalen, skal alle kostnader forbundet med revisjonen dekkes av Databehandler, herunder Behandlingsansvarliges og eksterne revisorers relevante kostnader.

12 VARIGHET OG OPPHØR

1. Databehandleravtalen gjelder fra den er signert med begge Parters underskrift og gjelder så lenge Databehandler behandler Personopplysninger på vegne av Behandlingsansvarlig i forbindelse med Hovedavtalen.
2. Behandlingsansvarlig kan ved brudd på Databehandleravtalen eller bestemmelsene i Gjeldende personvernregler pålegge Databehandler å stoppe den videre Behandlingen av Personopplysningene med øyeblikkelig virkning.
3. Ved opphør av Databehandleravtalen plikter Databehandler å slette eller tilbakelevere alle Personopplysninger som forvaltes på vegne av Behandlingsansvarlig og som omfattes av Databehandleravtalen. Dette gjelder også eventuelle sikkerhetskopier. Behandlingsansvarlig bestemmer hvordan tilbakelevering av Personopplysninger skal skje, herunder hvilket format som skal benyttes.
4. Databehandler skal skriftlig bekrefte og dokumentere at sletting er foretatt. Bekreftelsen skal gis innen 14 dager etter at sletting er gjennomført i henhold til vedlegg 1.

13 LOVVALG OG VERNETING

Databehandleravtalen er underlagt norsk rett og Partene vedtar Oslo tingrett som vernetting. Dette gjelder også etter opphør av Databehandleravtalen.

14 KONTAKTPERSONER

Alle meddelelser vedrørende Databehandleravtalen rettes skriftlig og adressert til følgende kontaktpersoner:

Hos Behandlingsansvarlig (NAV):

Inger Anderssen
Avdelingsdirektør
Inger.anderssen@nav.no

Hos Databehandler:

Navn
Stilling
e-post

15 VEDLEGG 1 DATABEHANDLINGENS OMFANG

Behandlingens formål

Gi en beskrivelse av hva som er formålet med behandlingen av personopplysninger hos Databehandler for å kunne utføre oppdrag eller tjeneste for NAV.

Arbeidsrettet rehabilitering skal bidra til å styrke tiltaksdeltakerens arbeidsevne og bidra til mestring av helserelaterte og sosiale problemer som kan være til hinder for deltakelse i arbeidslivet. Arbeidsrettet rehabilitering kan inneholde arbeidsforberedende trening, arbeidsutprøving, kontakt med arbeidslivet, generell opptrening, funksjonsfremmende trening, opplæring, motivasjon, trening i sosial mestring, livsstilsveiledning eller en kombinasjon av disse elementene.

Behandlingens art

Gi en beskrivelse eller sett inn referanse til relevante deler av Hovedavtalen eller vedlegg til Hovedavtalen som beskriver oppdraget eller tjenesten.

Personopplysningene skal brukes til å gjennomføre gruppeundervisning, en-til-en samtaler, kartleggingsverktøy og praktisk opplæring. Tiltaket foregår både på tilrettelagte arbeidsplasser og hos ordinære arbeidsgivere, tiltaket kan også foregå digitalt.

Oppdraget er i henhold til Avtale mellom NAV Tiltak Agder og tiltaksarrangør om gjennomføring av arbeidsmarkedstiltaket Arbeidsrettet rehabilitering med tilhørende kravspesifikasjoner, jmf. Forskrift om arbeidsmarkedstiltak kapittel 12 Arbeidsrettet rehabilitering.

Kategorier av registrerte

Gi en oppstilling av hvilke kategorier av enkeltpersoner som opplysningene er knyttet til.

- Tiltaksdeltakere
- Arbeidsgiver
- NAV-ansatte
- Brukers nærstående kun for Arbeidsrettet rehabilitering
- Brukers verge for Arbeidsrettet rehabilitering

Type Personopplysninger

Gi en oppstilling av hvilke personopplysninger som skal behandles av Databehandler,

- Navn
- Adresse
- Telefonnummer
- E-postadresse
- Fødsels- /personnummer
- Fødselsdato
- Stemme
- Bilde
- Brukernavn
- IP-adresse
- Opplysninger knyttet til arbeidserfaring og verv som normalt fremkommer av en cv, herunder arbeidsgiver og hvor lenge man har jobbet
- Sertifikater og kurs
- Utdanning, herunder fagbrev, delkompetanse, høyere utdanning, grunnskoleutdanning
- Opplysninger om personlige egenskaper og interesser
- Opplysninger om språkkunnskap
- Opplysninger om atferd som kan ha betydning for tiltaksgjennomføring og jobbmuligheter
- Sosiale eller personlige forhold som kan ha betydning for tiltaksgjennomføring og jobbmuligheter
- Stønadsopplysninger

Type særlige kategorier av Personopplysninger (hvis relevant)

Gi en oppstilling av hvilke særlige kategorier av Personopplysninger (tidligere kalt sensitive) som skal behandles av Databehandler.

- Helseopplysninger

Spesifikke sletteregler

List opp og spesifiser eventuelt hvilke personopplysninger som har spesifikke sletteregler, og som skal slettes av Databehandler underveis i behandlingen av personopplysninger på vegne av Behandlingsansvarlig.

Tiltaksarrangør skal slette personopplysninger om enkeltdeltakere så snart det ikke er behov for opplysningene og senest innen 12 uker etter at deltaker har sluttet i tiltaket.

Tiltaksarrangør er pliktig å påse at data slettes hos sine eventuelle underdatabehandlere når formålet med behandlingen opphører.

Tiltaksarrangør skal ikke oppfordre deltaker til å logge på med sin private profil på eksterne tjenester, hvor tiltaksarrangør ikke har kontroll over deltakers personopplysninger og kan kreve disse slettet på vegne av deltaker.

Bistand til Behandlingsansvarlig

Gi en beskrivelse av hva det forventes at databehandleren bistår med for å oppfylle de ulike typene av registrertes rettigheter.

Databehandler skal korrigere eller slette konkrete personopplysninger innen 48 timer etter at Behandlingsansvarlig har gitt skriftlig beskjed om dette.

Tiltaksarrangør har ansvar for å gi deltakeren informasjon om behandlingen, om deltakerens rett til innsyn, retting, sletting og begrensning, og hvordan dette skal gjennomføres i tiltaksperioden.

16 VEDLEGG 2 TEKNISKE OG ORGANISATORISKE SIKKERHETSTILTAK

>Vedlegg 2 skal fylles ut<

I vedlegg 2 bør de viktigste sikringstiltakene beskrives, eventuelt at det henvises til dokumenter, anskaffelsesbilag, sikkerhetsbilag eller publikasjoner som forklarer hvordan databehandleren arbeider med informasjonssikkerhet og hvilke sikkerhetstiltak som er etablert for denne tjenesten/leveransen.

Databehandler skal som et minimum gjennomføre alle de tiltak som er angitt eller henvist til nedenfor. Databehandler kan ikke uten skriftlig samtykke fra Behandlingsansvarlig gjøre endringer i disse tiltakene som reduserer graden av datasikkerhet. Databehandler skal kontinuerlig arbeide for å forbedre sikkerhetstiltakene og sørge for at de oppdateres i takt med den teknologiske utviklingen.

Pseudonymiseringstiltak

Pseudonymisering vil si behandling av personopplysninger på en slik måte at personopplysningene ikke lenger kan knyttes til en bestemt registrert uten bruk av tilleggsinformasjon, forutsatt at slik tilleggsinformasjon oppbevares separat og er gjenstand for tekniske og organisatoriske tiltak som sikrer at personopplysningene ikke kan knyttes til en identifiser eller identifiserbar person.

Krypteringstiltak

Kryptering er prosessen med koding av data på en slik måte at bare autoriserte personer har tilgang til opplysningene.

Av personvern- og sikkerhetshensyn kreves at e-postkommunikasjon mellom NAV og tiltaksarrangør krypteres med Microsoft 365 eller tilsvarende sikkerhet. Dette punktet må også ses i sammenheng med spesifikke sletteregler.

Følgende personopplysninger kan sendes på kryptert e-post med tilstrekkelig sikkerhet:

Personopplysninger om deltaker:

- Navn
- Fødselsdato
- Telefonnummer
- E-postadresse
- NAV-kontor-tilhørighet

Personopplysninger om NAV-veileder

- Navn
- Telefonnummer
- E-postadresse
- NAV-kontor-tilhørighet

Tiltak for å sikre Personopplysningenes fortrolighet (konfidensialitet)

Sett inn beskrivelse. Eksempler kan være tiltak for å kontrollere tilgang, og for å skille opplysningene fra opplysninger som Databehandler behandler på vegne av andre behandlingsansvarlige.

Tiltak for å sikre Personopplysningenes integritet

Sett inn beskrivelse. Et eksempel kan være tiltak for å overvåke endringer i opplysningene.

Tiltak for å sikre tilgjengeligheten til Personopplysningene

Sett inn beskrivelse. Et eksempel kan være backup-tiltak.

Tiltak for å sikre robusthet i behandlingssystemene og -tjenestene

Sett inn beskrivelse. Eksempler kan være tiltak for katastrofegjenoppretting og redundans.

Tiltak for fysisk sikring av lokaler hvor data behandles

Sett inn beskrivelse.

Testdata

Databehandler skal rette seg etter Behandlingsansvarliges gjeldende retningslinjer for bruk av testdata. Sett inn beskrivelse av ytterligere tiltak.

Andre datasikkerhetstiltak:

Sett inn beskrivelse, eller "ikke relevant".

F.eks beskrive sletterutiner, anonymiseringsteknikk og evt behandling av særlige kategorier av personopplysninger under dette punktet.

17 VEDLEGG 3 GODKJENTE UNDERDATABEHANDLERE

Selskapets og org.nr.	navn	Selskapets adresse	Geografisk Behandling (jf. punkt 2.2)	lokasjon for	Beskrivelse av hvilken type Behandling

Taushetsplikt

Forvaltningsloven, arbeids- og velferdsforvaltningsloven og lov om sosiale tjenester i arbeids- og velferdsforvaltningen inneholder strenge regler om taushetsplikt. Det skal bevares taushet om alle opplysninger en i medfør av arbeid for NAV får om noens personlige forhold.

Taushetsplikten gjelder også opplysninger som fødested, fødselsdato, personnummer, statsborgerforhold, sivilstand, yrke, bosted og arbeidssted. I tillegg vil taushetsplikten kunne omfatte opplysninger om drifts- eller forretningsforhold som det vil være av konkurransemessig betydning å hemmeligholde av hensyn til den opplysningen gjelder.

Taushetsplikten innebærer både at man skal unnlate å avsløre opplysninger for andre og aktivt hindre at uvedkommende får tilgang eller kjennskap til taushetsbelagte opplysninger.

Taushetsplikten gjelder også overfor andre som utfører arbeid for NAV med mindre det foreligger tjenstlige behov.

Taushetsplikten gjelder både i arbeidet og i fritiden. Taushetsplikten består også etter at tjeneste eller arbeid er utført. Opplysninger som er underlagt taushetsplikt, kan heller ikke utnyttes i egen virksomhet eller i tjeneste eller arbeid for andre.

Reglene om taushetsplikt gjelder alle som utfører arbeid for NAV. Alle plikter derfor å sette seg inn i reglene om taushetsplikt.

Alle som utfører arbeid for NAV, skal videre hindre at opplysninger om sikkerhetsrutiner og sikkerhetsinstruksjoner som regulerer NAVs sikkerhet gjøres kjent for uvedkommende.

Brudd på taushetsplikten kan medføre konsekvenser for det relevante kontraktuelle forhold og straffeansvar etter straffeloven §§ 209 og 210.

Denne erklæringen undertegnes digitalt sammen med databehandleravtalen.

Ved signatur bekrefter jeg å ha lest og forstått min taushetsplikt og har gjort meg kjent med de lovbestemmelsene som er sitert på de neste sidene.

SITAT FRA RELEVANTE LOVTEKSTER

De sentrale bestemmelsene finnes i forvaltningsloven §§ 13-13e og 13 g. For saker på arbeids- og velferdsetatens område er det i arbeids- og velferdsforvaltningsloven § 7 gitt regler som er strengere og kommer i tillegg til forvaltningsloven. Det samme gjelder lov om sosiale tjenester i arbeids- og velferdsforvaltningen § 44.

ARBEIDS- OG VELFERDSFORVALTNINGSLOVEN § 7, SITAT:

”Enhver som utfører tjeneste eller arbeid for Arbeids- og velferdsetaten etter denne loven, har taushetsplikt etter forvaltningsloven §§ 13 til 13 e og 13 g. Taushetsplikten gjelder også fødested, fødselsdato, personnummer, statsborgerforhold, sivilstand, yrke, bosted og arbeidssted. Det kan bare gjøres unntak fra taushetsplikten når dette følger av bestemmelsene i andre til femte ledd eller av andre bestemmelser gitt i eller i medhold av lov.

Opplysninger om en person kan brukes ved formidling av arbeid eller ved gjennomføring av arbeidsmarkedstiltak.

Det kan bare gis opplysninger til andre forvaltningsorganer etter forvaltningsloven § 13 b første ledd nr. 6 når det er nødvendig for å fremme Arbeids- og velferdsetatens oppgaver eller for å hindre at noen urettmessig får utbetalt offentlige midler eller unndrar midler fra innbetaling til det offentlige.

Taushetsplikten etter første ledd er ikke til hinder for at nødvendige opplysninger gis til Innkrevingssentralen for bidrag og tilbakebetalingskrav i tilknytning til krav som den krever inn på vegne av Arbeids- og velferdsetaten. Departementet kan i forskrift fastsette på hvilken måte opplysningene skal gis.”

FORVALTNINGSLOVEN § 13-13E OG 13G, SITAT:

”Enhver som utfører tjeneste eller arbeid for et forvaltningsorgan, plikter å hindre at andre får adgang eller kjennskap til det han i forbindelse med tjenesten eller arbeidet får vite om:

- 1) noens personlige forhold, eller
- 2) tekniske innretninger og fremgangsmåter samt drifts- eller forretningsforhold som det vil være av konkurransemessig betydning å hemmeligholde av hensyn til den som opplysningen angår.

Som personlige forhold regnes ikke fødested, fødselsdato og personnummer, statsborgerforhold, sivilstand, yrke, bopel og arbeidssted, med mindre slike opplysninger røper et klientforhold eller andre forhold som må anses som personlige. Kongen kan ellers gi nærmere forskrifter om hvilke opplysninger som skal regnes som personlige, om hvilke organer som kan gi privatpersoner opplysninger som nevnt i punktumet foran og opplysninger om den enkeltes personlige status for øvrig, samt om vilkårene for å gi slike opplysninger.

Taushetsplikten gjelder også etter at vedkommende har avsluttet tjenesten eller arbeidet. Han kan heller ikke utnytte opplysninger som nevnt i denne paragraf i egen virksomhet eller i tjeneste eller arbeid for andre”.

§ 13 a. (begrensninger i taushetsplikten når det ikke er behov for beskyttelse).

Taushetsplikt etter § 13 er ikke til hinder for:

1. at opplysninger gjøres kjent for dem som de direkte gjelder, eller for andre i den utstrekning de som har krav på taushet samtykker,
2. at opplysningene brukes når behovet for beskyttelse må anses varetatt ved at de gis i statistisk form eller ved at individualiserende kjennetegn utelates på annen måte, og
3. at opplysningene brukes når ingen berettiget interesse tilsier at de holdes hemmelig, f.eks. når de er alminnelig kjent eller alminnelig tilgjengelig andre steder.
4. at opplysninger om en navngitt domfelt eller botlagt er benådet eller ikke og hvilke reaksjoner vedkommende eventuelt blir benådet til, gjøres kjent.

§ 13 b. (begrensninger av taushetsplikten ut fra private eller offentlige interesser).

Taushetsplikt etter § 13 er ikke til hinder for:

1. at opplysningene i en sak gjøres kjent for sakens parter eller deres representanter,
2. at opplysningene brukes for å oppnå det formål de er gitt eller innhentet for, bl.a. kan brukes i forbindelse med saksforberedelse, avgjørelse, gjennomføring av avgjørelsen, oppfølging og kontroll,
3. at opplysningene er tilgjengelig for andre tjenestemenn innen organet eller etaten i den utstrekning som trengs for en hensiktsmessig arbeids- og arkivordning, bl.a. til bruk ved vegledning i andre saker,
4. at opplysningene brukes for statistisk bearbeiding, utrednings- og planleggingsoppgaver, eller i forbindelse med revisjon eller annen form for kontroll med forvaltningen,
5. at forvaltningsorganet gir andre forvaltningsorganer opplysninger om en persons forbindelse med organet og om avgjørelser som er truffet og ellers slike opplysninger som det er nødvendig å gi for å fremme avgiverorganets oppgaver etter lov, instruks eller oppnevningssgrunnlag,
6. at forvaltningsorganet anmelder eller gir opplysninger (jfr. også nr. 5) om lovbrudd til påtalemyndigheten eller vedkommende kontrollmyndighet, når det finnes ønskelig av allmenne omsyn eller forfølgning av lovbruddet har naturlig sammenheng med avgiverorganets oppgaver,
7. at forvaltningsorganet deler opplysningene med andre så langt det er nødvendig for å unngå fare for liv eller helse,

8. at forvaltningsorganet gir et annet forvaltningsorgan opplysninger (samordning) som forutsatt i lov om Oppgaverregisteret

9. at forvaltningsorganet gir et forvaltningsorgan i en annen EØS-stat opplysninger som forutsatt i tjenesteloven.

Part eller partsrepresentant som blir gjort kjent med opplysninger etter første ledd nr. 1, kan bare bruke opplysningene i den utstrekning det er nødvendig for å vareta partens tarv i saken.

Forvaltningsorganet skal gjøre ham merksam på dette. Likeledes kan forvaltningsorganet pålegge taushetsplikt når vitner o.l. får opplysninger undergitt taushetsplikt i forbindelse med at de uttaler seg til organet. Overtreding av taushetsplikt etter dette ledd kan straffes etter straffelovens § 209, dersom vedkommende er gjort merksam på at overtreding kan få slik følge.

§ 13 c. (informasjon om taushetsplikt, oppbevaring av opplysninger undergitt taushetsplikt)

Vedkommende forvaltningsorgan skal sørge for at taushetsplikten blir kjent for dem den gjelder, og kan kreve skriftlig erklæring om at de kjenner og vil respektere reglene.

Dokumenter og annet materiale som inneholder opplysninger undergitt taushetsplikt, skal forvaltningsorganet oppbevare på betryggende måte.

Kongen kan gi nærmere regler om oppbevaring av dokumenter og annet materiale som er undergitt taushetsplikt, om tilintetgjøring av dokumenter eller materiale og om bortfall av taushetsplikt etter en viss tid. Taushetsplikten bortfaller etter 60 år når ikke annet er bestemt i medhold av foregående punktum.

§ 13 d. (opplysninger til bruk for forskning)

Når det finnes rimelig og ikke medfører uforholdsmessig ulempe for andre interesser, kan departementet bestemme at et forvaltningsorgan kan eller skal gi opplysninger til bruk for forskning, og at dette skal skje uten hinder av organets taushetsplikt etter § 13.

Til vedtak som nevnt i første ledd kan det knyttes vilkår. Disse kan bl.a. gi bestemmelser om hvem som skal ha ansvar for opplysningene og hvem som skal ha adgang til dem, om oppbevaring og tilbakelevering av utlånt materiale, om tilintetgjøring av avskrifter, om hvorvidt forskerne skal ha adgang til å henvende seg til eller innhente nærmere opplysninger om dem det er gitt opplysninger om, og om bruken av opplysningene for øvrig.

Kongen kan gi nærmere forskrifter om vedtak etter denne paragraf.

§ 13 e. (forskeres taushetsplikt).

Enhver som utfører tjeneste eller arbeid i forbindelse med en forskingsoppgave som et forvaltningsorgan har støttet, godkjent eller gitt

opplysninger undergitt taushetsplikt til, plikter å hindre at andre får adgang eller kjennskap til:

1. opplysninger undergitt taushetsplikt som forskeren får fra et forvaltningsorgan,

2. opplysninger som i forbindelse med forskningsarbeidet er mottatt fra private under taushetsløfte, og

3. opplysninger som gjelder personer som står i et avhengighetsforhold til den instans (skole, sykehus, anstalt, bedrift, offentlig myndighet m.m.) som har formidlet deres kontakt med forskeren.

Opplysningene kan bare brukes slik det er nødvendig for forskingsarbeidet og i samsvar med de vilkår som måtte være fastsatt etter § 13 d annet ledd. Skal resultater av forskingsarbeidet publiseres eller brukes på annen måte, gjelder § 13 a nr. 1 og 2 tilsvarende.

Brudd på taushetsplikten eller på vilkår etter § 13 d annet ledd, straffes etter straffelovens § 209.

Departementet eller vedkommende forvaltningsorgan skal gjøre forskeren og hans medarbeidere kjent med taushetsplikten og straffebestemmelsen, jfr. også § 13 c første ledd.”

§ 13 g. (Forskrift om adgang til informasjonsdeling og annen behandling av taushetsbelagte opplysninger)

Kongen kan gi forskrift om at taushetsplikt etter § 13 ikke skal være til hinder for at bestemte organer kan dele opplysninger for å utføre oppgaver som er lagt til avgiver- eller mottakerorganet, så langt delingen ikke utgjør et uforholdsmessig inngrep overfor den opplysningene gjelder, og om annen behandling av opplysninger i forbindelse med delingen. Der det foreligger et etablert samarbeid mellom organer, kan forskrifter etter første punktum om nødvendig også omfatte opplysninger som etter annen lov er underlagt særlige begrensninger i adgangen til å dele opplysninger etter § 13 b første ledd.

STRAFFELOVEN §§ 209 OG 210, SITAT:

§209. Brudd på taushetsplikt
”Med bot eller fengsel inntil 1 år straffes den som krenker taushetsplikt som han eller hun har i henhold til lovbestemmelse eller forskrift, eller utnytter en opplysning han eller hun har taushetsplikt om med forsett om å skaffe seg eller andre en uberettiget vinning.

Første ledd gjelder tilsvarende ved brudd på taushetsplikt som følger av gyldig instruks for tjeneste eller arbeid for statlig eller kommunalt organ.

For den som arbeider eller utfører tjeneste for et statlig eller kommunalt organ, rammer første og annet ledd også brudd på taushetsplikt etter at tjenesten eller arbeidet er avsluttet.

Grovt uaktsom overtredelse straffes på samme måte.

Medvirkning er ikke straffbar.”

§ 210. Grovt brudd på taushetsplikt

”Grovt brudd på taushetsplikt straffes med fengsel inntil 3 år.

Ved avgjørelsen av om taushetsbruddet er grovt skal det særlig legges vekt på om gjerningspersonen har hatt forsett om uberettiget vinning og om handlingen har ført til tap eller fare for tap for noen”.

LOV OM SOSIALE TJENESTER I ARBEIDS OG VELFERDSFORVALTNINGEN § 44, SITAT:

”Enhver som utfører tjeneste eller arbeid for kommunen etter denne loven, har taushetsplikt etter forvaltningsloven §§ 13 til 13 e og 13 g.

Overtredelse straffes etter straffeloven § 209.

Taushetsplikten gjelder også fødested, fødselsdato, personnummer, statsborgerforhold, sivilstand, yrke, bopel og arbeidssted. Opplysning om en tjenestemottakers oppholdssted kan likevel gis når det er klart at det ikke vil skade tilliten til kommunen.

Det kan bare gis opplysninger til andre forvaltningsorganer etter forvaltningsloven § 13 b nr. 6 når dette er nødvendig for å fremme kommunen i arbeids- og velferdsforvaltningens oppgaver.

Uten hinder av taushetsplikten kan kommunen etter forespørsel utlevere tjenestemottakerens kontaktopplysninger og opplysninger om mulig oppholdssted til politiet og kriminalomsorgen til bruk i deres tjeneste.

Dersom et barns interesser tilsier det, kan fylkesmannen eller departementet bestemme at opplysninger skal være undergitt taushetsplikt, selv om foreldrene har samtykket i at de gjøres kjent.

