

Veileder til tiltaksarrangør for utfylling av databehandleravtale

Innledning

Nav har utarbeidet en mal for databehandleravtale. Databehandleravtalen består av ett hoveddokument og tre vedlegg:

- **Vedlegg 1** inneholder en beskrivelse av *behandlingsens omfang, formål, art, type personopplysninger, kategorier av registrerte og varighet av behandlingen*.
- **Vedlegg 2** skal beskrive de *tekniske og organisatoriske tiltakene* som databehandler og underdatabehandlere gjør.
- **Vedlegg 3** er en oppstilling av alle *godkjente underdatabehandlere*. Her skal dere fylle ut informasjon om selskapene og behandlingen av personopplysninger.

Hoveddokumentet og vedlegg 1 fylles ut av Nav. Vi ber om at dere fyller ut vedlegg 2 og vedlegg 3, for å sikre en fullstendig oversikt over underdatabehandlere, samt å sikre at tiltakene er noe dere har mulighet til å iverksette.

Nedenfor følger en veileder for hvordan vi ønsker at vedlegg 2 og vedlegg 3 fylles ut. Vi anbefaler å starte med å fylle ut vedlegg 3.

Utfylling av vedlegg 3

Her skal dere liste opp alle underdatabehandlere som behandler personopplysninger på vegne av Nav. Dette kan være forskjellige typer verktøy og programmer, for eksempel et fagsystem eller et tekstbehandlingsprogram.

Utfylling av tabell

Selskapets navn og organisasjonsnummer

Her skal dere fylle ut navn og org.nr. på selskapet, samt navn på applikasjon og/eller skytjeneste som benyttes.

Dersom dere eksempelvis bruker Word til å notere personopplysninger, skal dere presisere om dere bruker skytjeneste eller en lokal løsning.

Selskapets adresse

Her skal dere fylle ut selskapets adresse, samt adressen til selskapets hovedkontor hvis disse er ulike.

Geografisk lokasjon for behandling

Her skal dere fylle ut det geografiske stedet hvor behandling av personopplysninger foregår. Her må dere inkludere alle steder hvor den aktuelle underleverandøren behandler personopplysninger. Dette innebærer:

- Lagringssted
- Lokasjon for support-personell

- Lokasjon for personell med administrator-tilgang
- Lokasjon for teknisk support-personell

Beskrivelse av hvilken type behandling

Her skal dere fylle ut:

- **Hva** behandlingen går ut på (f.eks. fagsystem for å kommunisere med deltaker)
- **Hvem** det behandles personopplysninger om (f.eks. deltakere, Nav-ansatte)
- **Hvilke** personopplysninger som behandles i det aktuelle systemet (f.eks. navn, fødselsnummer og bilde)

Eksempel på utfylling

Dette er et eksempel på hvordan tabellen kan fylles ut. Alt innhold i tabellen er fiktivt, og er kun ment som en illustrasjon.

Selskapets navn og org.nr.	Selskapets adresse	Geografisk lokasjon for Behandling (jf. punkt 2.2)	Beskrivelse av hvilken type Behandling
Karriereforalle AS Org.nr. 123 45 678	Nordre veg 1. 1111 Oslo	Lagringssted: Norge Supportsted: Sverige Teknisk support: Irland	Karriereverktøy som brukes til kartlegging av deltakers kompetanse. Det behandles personopplysninger om deltakere. Personopplysninger om deltaker som behandles: Navn, epost, telefonnummer.
Tekstogtall AS Org.nr. 234 56 789	Søndre veg 2, 2222 Bergen	Lagringssted: EU Supportsted: Norge Administratortilgang/Teknisk support: Norge	Tekstbehandling som brukes til samtalereferat med deltakere. Det behandles personopplysninger om deltakere og Nav-ansatte. Personopplysninger om deltaker som behandles: Navn, arbeidserfaring, opplysninger om personlige egenskaper og interesser.

		Personopplysninger om Nav-ansatte som behandles: Navn, e-postadresse.
--	--	---

Utfylling av vedlegg 2

I vedlegg 2 skal dere fylle ut hvilke *tekniske og organisatoriske sikkerhetstiltak* både dere selv og deres underdatabehandlere gjør, for å sikre de registrertes personvern. Her skal dere forklare hvordan dere som databehandler, og de enkelte underdatabehandlerne dere benytter, arbeider med informasjonssikkerhet, og hvilke sikkerhetstiltak som er etablert for de ulike tjenestene. Vi trenger en beskrivelse av tiltakene som gjennomføres, for å kunne vurdere om sikkerhetsnivået er egnet med hensyn til risikoen.

Med underdatabehandlere mener vi alle andre systemer, programmer, tjenester e.l. som dere som databehandler benytter dere av på en måte som innebærer å behandle personopplysninger på vegne av Nav. Dette kan for eksempel være CRM-system, læringsplattformer, tekstbehandlingsprogram, saksbehandlingsverktøy, spill, support, skylagringstjeneste, med flere.

I tabellen under hvert tiltak skal dere føre inn samtlige underdatabehandlere som er oppført i vedlegg 3. I høyre kolonne skal dere beskrive hvilke tiltak som gjøres hos den enkelte databehandleren. Det kan også vises til arkiverte dokumenter, anskaffelsesbilag, sikkerhetsbilag eller publikasjoner som forklarer hvordan databehandleren arbeider med informasjonssikkerhet og hvilke sikkerhetstiltak som er etablert for denne tjenesten. Det skal ikke brukes lenker, da informasjonen man finner på siden det lenkes til vil kunne endre seg.

Hvis et tiltak ikke er aktuelt for en databehandler, kan dere føre inn “ikke aktuelt”, samt en kort forklaring på hvorfor det ikke er aktuelt for denne databehandleren.

Listen er ikke uttømmende, slik at hvis dere gjennomfører flere sikkerhetstiltak, skal dere oppføre disse under siste punkt (“Andre sikkerhetstiltak”).

Eksempel på utfylling

Dette er et eksempel på hvordan vedlegget kan fylles ut. Alt innhold er fiktivt og forenklet, og er kun ment som en illustrasjon på ønsket oppsett.

Pseudonymiseringstiltak

Pseudonymisering vil si å behandle personopplysninger på en slik måte at personopplysningene ikke lenger kan knyttes til en bestemt registrert uten bruk av tilleggsinformasjon. En forutsetning er at slik tilleggsinformasjon oppbevares separat og

er gjenstand for tekniske og organisatoriske tiltak som sikrer at personopplysningene ikke kan knyttes til en identifisert eller identifiserbar person.

Et eksempel på pseudonymiseringstiltak er å benytte et separat program for å opprette og administrere løpenumre, for deretter utelukkende å benytte løpenummer som identifikasjonsfaktor ved behandling av personopplysninger i andre sammenhenger.

Databehandler	Pseudonymiseringstiltak
Karriereforalle (Underdatabehandler 1)	Journalnotater knyttes utelukkende til løpenummer opprettet i Tekstogtall for identifikasjon, uten bruk av navn, initialer eller andre identifikasjonsfaktorer.
Tekstogtall (Underdatabehandler 2)	Programmet benyttes til å opprette løpenummer til bruk i andre systemer. Løpenummeret knyttes til deltakers navn og fødselsdato.

For å få plass til flere underdatabehandlere i tabellen, høyreklikk på tabellen, trykk på «sett inn» og velg om du ønsker ny rad under eller over den raden du jobber i for øyeblikket, eller hold musepekeren over den nederste linjen i tabellen og trykk på det lille plussikonet som kommer opp i venstre hjørne.

Krypteringstiltak

Kryptering er prosessen med koding av data på en slik måte at bare autoriserte personer har tilgang til opplysningene. Krypteringen er en slags «nøkkel», som låser ned informasjonen slik at den ikke kan leses frem til den låses opp igjen med riktig «nøkkel».

Eksempler på kryptering er TLS-kryptering av dataoverføringer (f.eks. e-post eller lynmeldinger) og https-protokollen (basert på TLS-kryptering) for kryptering av nettsteder.

I tabellen fyller dere ut hvilke metoder og teknologier som benyttes internt hos dere, og hos underdatabehandlere, for kryptering av filer, kommunikasjon, dataoverføringer og lagring av personopplysninger m.m.

Databehandler	Krypteringstiltak
Tiltaksarrangør ABC (Databehandler)	<ul style="list-style-type: none">Dersom det produseres enkeltfiler som må sendes i e-post krypteres disse i PDF, og krypteringsnøkkelen sendes i separat SMS til mottakeren.All e-postkommunikasjon som omhandler tiltaket eller tiltaksdeltakere krypteres med krypteringsfunksjonen i e-postprogram A.
Karriereforalle (Underdatabehandler 1)	<ul style="list-style-type: none">All kommunikasjon mellom nettleser og servere er kryptert ved hjelp av TLS (https-protokollen).

	<ul style="list-style-type: none"> • Passord for tilgang til systemet er kryptert og saltet • Vi benytter abc-beskyttelse til kryptering av e-post. • Vi krypterer enkeltfiler i PDF og sender krypteringsnøkkelen separat på SMS til mottakeren.
Tekstogtall (Underdatabehandler 2)	Databasen er lagret på et filsystem som er kryptert etter 123-standard.

Tiltak for å sikre personopplysningenes fortrolighet (konfidensialitet)

Å sikre personopplysningenes fortrolighet og konfidensialitet handler om å sikre at informasjon bare er tilgjengelig for den som skal ha tilgang til den. Dette omfatter blant annet å sørge for at opplysningene lagres sikkert, er beskyttet mot uautorisert tilgang og ikke forveksles med andres opplysninger.

Eksempler på dette kan være tilgangsstyring, forskjellige innlogginger eller systemer for opplysninger som behandles på vegne av forskjellige behandlingsansvarlige eller adskilte servere eller nettverk for behandling av personopplysninger.

Databehandler	Tiltak for å sikre fortrolighet/konfidensialitet
Titaksarrangør ABC (Databehandler)	Ansatte hos oss er koblet på et sikret nettverk som er adskilt fra internettforbindelsen som benyttes av tiltaksdeltakere og gjester.
Karriereforalle (Underdatabehandler 1)	Veileder har kun tilgang til journalnotater tilknyttet egne brukere. Kun leder har tilgang til å endre veiledernes tilganger. Journalnotatene knyttet til løpenummer er delt i grupper for å skille brukere Nav er behandlingsansvarlig for, fra brukere tilhørende andre behandlingsansvarlige. Dette for å forhindre at veiledere for andre grupper får tilgang til journaler til Navs brukere. All tildeling og endring av tilgang loggføres, inkludert dersom leder gir seg selv tilgang til opplysninger.
Tekstogtall (Underdatabehandler 2)	Som standard er det kun veileder som har opprettet løpenummeret som har tilgang til opplysningene løpenummeret er koblet mot. Systemadministratorer, for tiden IT-ansvarlig, daglig leder og leder for tiltak A, kan gi en annen veileder tilgang i tilfelle fravær. Systemadministratorer har ikke direkte tilgang til opplysninger uten først å gi seg selv tilgang til opplysningene. All tildeling og endring av tilgang loggføres.

Tiltak for å sikre personopplysningenes integritet

Å sikre personopplysningenes integritet vil si å sikre at personopplysningene er riktige. Dette innebærer å hindre at opplysningene blir utilsiktet eller uautorisert endret eller slettet. Et eksempel på sikring av personopplysningenes integritet er loggføring av utførte endringer, som minst inkluderer tidspunktet for endring, hvem som utførte endringen, samt hvilken endring som ble gjort. Det bør også finnes rutiner for kontroll av loggene, for eksempel ved mistanke om utilsiktet endring, gjennomføring av stikkprøver eller rutinemessige kontroller.

Databehandler	Tiltak for å sikre integritet
Karriereforalle (Underdatabehandler 1)	Karriereforalle har en logg knyttet opp til den enkelte deltaker. Her blir alle endringer som gjøres på deltakerens profil loggført, med hvilken endring som ble utført, hvem som utførte endringen, og når endringen ble utført. Ledere har tilgang til å sjekke loggene. Loggen kan ikke slettes.
Tekstogtall (Underdatabehandler 2)	Vi har en rutine på at den registrerte får innsyn i egne personopplysninger, og kan deretter kreve endring eller sletting.

Tiltak for å sikre tilgjengeligheten til personopplysningene

Å sikre personopplysningenes tilgjengelighet vil si å sørge for at personopplysningene er tilstrekkelig og tidsnok tilgjengelige for det formålet de er samlet inn for. Det skal være mulig å gjenfinne personopplysningene til bruk for formålet innen rimelig tid selv om det oppstår uforutsette hendelser, for eksempel ved dataangrep eller at en datamaskin blir stjålet eller slutter å fungere.

Rutiner for sikkerhetskopier er et eksempel på tiltak for å sikre tilgjengelighet.

Databehandler	Tiltak for å sikre tilgjengelighet
Karriereforalle (Underdatabehandler 1)	Det kjøres rullerende sikkerhetskopier av hele databasen to ganger daglig, samt fullstendige sikkerhetskopier hver andre uke.
Tekstogtall (Underdatabehandler 2)	Alle lagrede data blir sikkerhetskopiert to ganger i døgnet.

Tiltak for å sikre robusthet i behandlingssystemene og -tjenestene

Å sikre robusthet i behandlingssystemer og -tjenester handler om å sørge for at systemet eller tjenesten er motstandsdyktig for sårbarheter, angrep og uhell. Eksempler er systemer for katastrofegjenoppretting og redundans.

Databehandler	Tiltak for å sikre robusthet
Karriereforalle (Underdatabehandler 1)	Ikke aktuelt. Det gjøres ingen ytterligere tiltak for å sikre robusthet utover backuptiltak.
Tekstogtall (Underdatabehandler 2)	Sikkerhetskopier blir lagret på to separate servere. Serverne er fysisk adskilt på to forskjellige steder i Norge, slik at risikoen for at begge blir satt ut av spill samtidig er minimert. Annenhver sikkerhetskopi lastes opp på de to forskjellige serverne, slik at den lagrede informasjonen på begge serverne er maks et døgn gammel.

Tiltak for fysisk sikring av lokaler hvor data behandles

Her ønsker vi en beskrivelse av fysiske sikringstiltak som er gjort på de fysiske lokasjonene der data behandles, slik som arbeidssteder, supportsteder eller lagringssteder. Det kan også vises til standarder for sikkerhetssertifisering dersom underdatabehandlere har slik sertifisering.

Eksempler på sikringstiltak kan være kameraovervåkning, inngjerdet område, elektronisk adgangskontroll med behovsbaserte tilganger og soneinndeling med adgangskontroll av lokaler som benyttes til flere ting enn bare behandling av personopplysninger.

Databehandler	Tiltak for fysisk sikring
Tiltaksarrangør ABC (Databehandler)	Kontordelen av bygget er sikret med elektronisk adgangskontroll med kort og kode.
Karriereforalle (Underdatabehandler 1)	Kontorbygningen for drift, utvikling og support er kameraovervåket og har dobbel elektronisk adgangskontroll for ytre skall og selve kontorområdet. Serverne der data er lagret er plassert i en bygning med kameraovervåkning og elektronisk adgangskontroll med tofaktorautentisering som benytter seg av brikke og biometri. Bygningen ligger på et inngjerdet område som også er kameraovervåket på inn- og utside, samt døgntkontinuerlig vekterpatruljering og elektronisk adgangskontroll med krav om forutgående innmelding av besøk på området.
Tekstogtall (Underdatabehandler 2)	Serverne er plassert i en serverpark som er sertifisert etter ISO123-standarden. Support er basert i egen bygning med fysisk og elektronisk adgangskontroll. Kontorbygningen for drift og utvikling har kameraovervåkede innganger og elektronisk adgangskontroll med kort og kode.

Tiltak for å sikre anonymisering ved datauttrekk til statistiske formål

Under dette punktet skal dere liste opp hvilke personopplysninger som benyttes til statistiske formål, og hvordan disse blir anonymisert. Nav tillater kun bruk av personopplysninger til statistikkformål dersom personopplysningene anonymiseres før de benyttes i statistikk.

Det presiseres at databehandler må ha et gyldig formål og behandlingsgrunnlag for selve prosessen med å anonymisere personopplysninger til statistiske formål, ettersom dette i seg selv utgjør en behandling av personopplysninger. Formålet og behandlingsgrunnlaget for rapportering til Nav er beskrevet i Vedlegg 1. Ønsker databehandler å levere statistikk til andre aktører, f.eks. sine bransjeorganisasjoner, må formål og behandlingsgrunnlag beskrives her, slik at vi kan ta det inn i Vedlegg 1.

Det er en forutsetning at opplysningene som skal anonymiseres er samlet inn og behandlet i samsvar med gjeldende databehandleravtale. Å behandle personopplysninger som ikke er angitt i databehandleravtalens vedlegg 1 vil være et brudd på databehandleravtalen, også ved behandling til statistiske formål.

I tabellen under er det oppført eksempler på parametere som databehandler kan ønske å beholde (kjønn, fødselsår, sluttårsak, arbeidsgiver, helseutfordringer). Disse må skiftes ut med de parameterne som databehandler ønsker å beholde i det konkrete tilfellet.

Parameter	Beskrivelse
Eksempel 1: Kjønn	Ikke aktuelt.
Eksempel 2: Fødselsår	Beskriv hvilke spesifikke parametere som beholdes. For eksempel aldersspenn 20-30 år eller eksakt alder.
Eksempel 3: Sluttårsak	Beskriv hvilke spesifikke parametere som beholdes, f.eks. overgang til arbeid ja/nei eller om også overgang til fast ytelse, videre oppfølging hos Nav e.l. er tatt med
Eksempel 4: Arbeidsgiver	Beskriv hvilke spesifikke parametere som beholdes, f.eks. navn på arbeidsgiver eller kun bransjetilhørighet
Eksempel 5: Helseutfordringer	Beskriv hvilke spesifikke parametere som beholdes, f.eks. ja/nei eller kronisk/forbigående

Informasjon om anonymisering	
Når i tiltaksgjennomføringen blir opplysningene anonymisert?	
Hvordan foregår selve anonymiseringsprosessen?	

Hvem har tilgang til opplysningene før de blir anonymisert/hvem gjennomfører anonymiseringen?	
Hvilke systemer behandler personopplysninger til statistikk og analyseformål?	

Tiltak for å sikre sletting av personopplysninger

Her skal dere beskrive sletterutiner for personopplysninger dere behandler på vegne av Nav, for alle kategorier registrerte. For eksempel ønsker vi en beskrivelse av rutiner for sletting av personopplysninger etter tiltaksslutt, og rutiner for sletting av personopplysninger for deltakere som ikke begynner i tiltaket, eller som avslutter underveis.

Databehandler	Tiltak for å sikre sletting
Karriereforalle (Underdatabehandler 1)	Alle opplysninger tilknyttet en deltaker slettes fra systemet 8 uker etter avsluttet tiltaksdeltakelse. Backup går 4 uker tilbake, og det er dermed sikret at det etter 12 uker ikke vil være mulig å gjenskape informasjon fra database eller backup.
Tekstogtall (Underdatabehandler 2)	Alle personopplysninger slettes 4 uker etter avsluttet tiltaksdeltakelse. Backup går 6 uker tilbake, og innen 10 uker vil dermed alle opplysninger i database og backup være slettet.
Tiltaksarrangør ABC (Databehandler)	Hver enkelt veileder har selv ansvar for sletting av lagrede opplysninger på sin jobbtelefon og e-post så snart formålet er oppnådd eller opplysningene er overført til egnet fagsystem.

Andre datasikkerhetstiltak

Dersom dere eller underdatabehandlere har iverksatt andre datasikkerhetstiltak som ikke er beskrevet under punktene over, skal disse beskrives her.

Eksempel på dette kan være adskilte nettverk for ansatte og tiltaksdeltakere/gjester.

Databehandler	Tiltak
Tiltaksarrangør ABC (Databehandler)	Ansatte benytter eget sikret nettverk innenfor kontorsonen. Tilgang til underdatabehandleres systemer er betinget tilkobling til dette nettverket, slik at datamaskiner som er utenfor kontorsonen og dennes adgangskontroll ikke har kontakt med systemer det behandles personopplysninger i.