

**AVTALE OM BEHANDLING AV PERSONOPPLYSNINGER I DE  
DIGITALE TJENESTENE FOR DE KOMMUNALE SOSIALE  
TJENESTENE**

Databehandleravtale

mellom

[kommunenavn]  
som behandlingsansvarlig

og

Arbeids- og velferdsdirektoratet  
som databehandler

For Behandlingsansvarlig

For Databehandler (NAV)

Jan Erik Grundtjernlien

\_\_\_\_\_  
Behandlingsansvarlig

\_\_\_\_\_  
Databehandler (NAV)

Sted, dato

Avtalen undertegnes i to eksemplarer, ett til hver part.

---

## INNHALDSFORTEGNELSE:

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

---

---

## 1 FORMÅLET MED DENNE DATABEHANDLERAVTALEN

1. Denne avtalen ("databehandleravtalen") er en del av samarbeidsavtale om digitale tjenester for de kommunale sosiale tjenestene ("samarbeidsavtalen") mellom [kommunenavn] («behandlingsansvarlig») og NAV («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 samarbeidsavtalen.
4. I tilfelle uoverensstemmelse mellom samarbeidsavtalen og databehandleravtalen når det gjelder forhold spesifikt knyttet til personvern, skal databehandleravtalen gis forrang.
5. Databehandleravtalen har tre vedlegg. Vedleggene er en del av databehandleravtalen. I tilfelle uoverensstemmelse mellom databehandleravtalen og vedleggene, skal vedleggene gis forrang.
6. Vedlegg 1 inneholder en beskrivelse av Behandlingens omfang, formål, art, type Personopplysninger, kategorier av registrerte og varighet av Behandlingen.
7. Vedlegg 2 inneholder en beskrivelse av tekniske og organisatoriske sikkerhetstiltak.
8. 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, lokaliseringsoplysninger, 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 samarbeidsavtalen.
  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.

## 5 BISTAND TIL BEHANDLINGSANSVARLIG

1. Databehandler plikter, så langt som mulig, 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 så snart som mulig 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 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 å 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. 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. Behandlingsansvarlig gir databehandler ved signering av denne avtalen en generell godkjenning til bruk av underdatabehandlere. Databehandler kan ved behov gjøre endringer i bruken av underdatabehandlere forutsatt at behandlingsansvarlig underrettes og gis mulighet til å motsette seg endringene. Behandlingsansvarlig skal gis 30 dagers varsel om endring av underdatabehandlere. Dersom behandlingsansvarlig motsetter seg databehandlers endring av underdatabehandler, er behandlingsansvarlig forpliktet til å fremlegge skriftlig redegjørelse og dokumentasjon på at det foreligger saklig grunn til å motsette seg endringen innen 14 dager etter at varsel er mottatt fra databehandler. Partene skal sammen forsøke å komme frem til en omforent løsning. Dersom partene ikke blir enige, kan behandlingsansvarlig avslutte den berørte delen av tjenesten. 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.
  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. Databehandler har fullt ansvar for underdatabehandlers utførelse av sine forpliktelser på samme måte som om databehandler selv sto for utførelsen.

## 9 OVERFØRING AV PERSONOPPLYSNINGER TIL TREDJESTAT

1. Databehandler skal lagre personopplysninger i EU/EØS og forhåndsgodkjente tredjeland. Når det er nødvendig for å gjennomføre oppdrag/tjeneste som omfattes av databehandleravtalen, kan databehandler overføre personopplysninger til et tredjeland. Slik overføring skal alltid skje i overensstemmelse med GDPR kapittel V. Overføringsgrunnlag spesifiseres i vedlegg 3.
2. Unntak kan også 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 etter at databehandler ble oppmerksom på bruddet, slik at behandlingsansvarlig har mulighet til å melde bruddet til Datatilsynet innenfor tidsfristen på 72 timer.

## 11 REVISJON

1. Databehandler skal dokumentere og kunne 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. Slik revisjon kan gjennomføres én gang per år, ikke tidligere enn 30 dager etter at behandlingsansvarlig har gitt skriftlig beskjed til databehandler og først etter at partene er kommet til enighet om en gjennomføringsdato. Revisjonen skal foregå innenfor normal arbeidstid og ikke forstyrre databehandlers virksomhet unødvendig. 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. Behandlingsansvarlig kan få oversendt kopi av revisjonsrapporter på forespørsel. Behandlingsansvarlig skal ha rett til å fremlegge slike revisjonsrapporter til sine eksterne revisorer og tilsynsmyndigheter.
  4. Hver av partene dekker sine egne kostnader forbundet med en revisjon.
-

---

## 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 samarbeidsavtalen.
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, med mindre videre behandling er lovpålagt. Dette gjelder også eventuelle sikkerhetskopier.

## 13 LOVVALG OG VERNETING

Databehandleravtalen er underlagt norsk rett og partene vedtar Oslo tingrett som verneting. Dette gjelder også etter opphør av databehandleravtalen.

---



---

## VEDLEGG 1 DATABEHANDLINGENS OMFANG

### Behandlingens formål

Arbeids- og velferdsdirektoratet skal etter samarbeidsavtalen tilby digitale tjenester for de kommunale sosiale tjenestene. Partene samarbeider om å utvikle nye og eksisterende digitale tjenester for innbyggerne fortløpende. Hensikten er å gi bedre service og tjenester til kommunens innbyggere, muligheten til å søke om økonomisk sosialhjelp digitalt, og sette NAV-kontoret i stand til å komme raskere i gang med søknadsbehandlingen.

For å levere digitale tjenester til kommunens innbyggere, er det nødvendig for Arbeids- og velferdsdirektoratet å behandle enkelte personopplysninger om innbyggerne på vegne av kommunen.

### Behandlingens art

De digitale tjenestene omfatter: Digital søknad om økonomisk sosialhjelp, og innsyn til bruker via nav.no (innsynsløsningen), innsynsflate for NAV Kontaktsenter (veilede innbyggere som kontakter NAV), digital klage for økonomisk sosialhjelp. Tjenesten skal kontinuerlig videreutvikles der det er hensiktsmessig for bruker, kommunen og AvDir. Se samarbeidsavtalen punkt 3.

Arbeids- og velferdsdirektoratet benytter GCP (Google Cloud Platform) som dataplattform for applikasjonene som benyttes i de digitale løsningene. Dette innebærer at personopplysningene som behandles i dagens løsninger, vil behandles i GCP.

### Digital søknad om økonomisk sosialhjelp

Digital søknad gir innbygger mulighet til å søke om økonomisk sosialhjelp digitalt fra nav.no. Når innbyggeren velger å bruke den digitale søknaden, hentes det automatisk inn personopplysninger fra systemer NAV har tilgang til, og innbyggeren har i tillegg mulighet til å gi de opplysningene innbyggeren ønsker.

Opplysningene i søknaden brukes i saksbehandlingen av søknaden i den enkelte kommunen som søknaden er sendt til. Oppholdsadresse benyttes for å vite hvilken kommune søknaden skal sendes til og som er behandlingsansvarlig for søknaden.

Noe metadata lagres slik at innbyggeren kan se spor av forsendelsen på nav.no i ettertid. Egne sletteregler ligger til grunn.

### Innsynsløsning for innbyggeren

Løsningen gir mottaker av økonomisk sosialhjelp mulighet til å følge med på status i søknaden sin, egen saksgang og utbetalinger.

Personopplysningene som hentes inn i innsynsløsningen skal brukes for å kunne gi riktig person tilgang til sine søknader og pågående saker. Opplysningene skal også gi relevant informasjon for søkeren slik at de har oversikt i det som skjer knyttet til hver enkelt søknad de har på nav.no. Personopplysningene hentes fra PDL (persondataløsningen i NAV) og kommunalt fagsystem via KS sine tjenester.

---

### Innsynsflate for NAV Kontaktsenter

Innsynsflaten gir veiledere på sosiale tjenester hos NAV Kontaktsenter muligheten til å få tilgang til sentrale stønadsopplysninger i hver enkelt søknad. Oppslag i innsynsflaten gjøres kun når innbyggeren kontakter NAV Kontaktsenter per telefon.

Personopplysningene som hentes inn i innsynsflaten, skal brukes til å gi veiledere på sosiale tjenester hos NAV Kontaktsenter muligheten til å besvare generelle henvendelser fra innbyggeren i den enkelte kommune. Dette følger kanalstrategien til NAV, hvor NAV Kontaktsenter er førstelinje også for kommunene for de sosiale tjenestene.

### Innsiktsarbeid/målinger

For å kunne levere gode digitale tjenester ref. samarbeidsavtalen, er Arbeids- og velferdsdirektoratet avhengig av å gjøre innsiktsarbeid og foreta målinger på hvordan de digitale løsningene brukes. For å gjøre dette, er det nødvendig å behandle enkelte personopplysninger om innbyggere som besøker kommunale sider på nav.no.

### **Behandlinger som omfattes av Avtalen:**

Behandling		Behandlingsaktiviteter
Innsamling	Ja	NAV samler inn personopplysninger fra systemer og søkeren selv, for å kunne oversende søknader og relevant dokumentasjon fra nav.no til kommunalt fagsystem via KS FIKS.  NAV mottar personopplysninger fra kommunalt fagsystem for å kunne vise relevant informasjon om saksbehandlingen til søkeren, og NAV Kontaktsenter som førstelinje.
Registrering	Nei	
Lagring	Ja	NAV lagrer søknader frem til de er mottatt av kommunalt fagsystem, og påbegynte søknader på nav.no inntil 14 dager.  NAV lagrer metadata, generert på bakgrunn av innsendte søknader.
Strukturering	Ja	NAV strukturerer personopplysninger som hentes fra systemer og fra søkeren selv, i oversendelsen av søknader til kommunen via KS FIKS.  NAV viser strukturerte personopplysninger mottatt fra kommunalt fagsystem via KS FIKS.
Organisering	Nei	

Tilpasning eller endring	Ja	NAV konverterer opplastet dokumentasjon på vegne av søkeren for å gi muligheten til å sende inn flere typer dokumenter. Ved at søkeren velger å sende inn dokumentasjon, godtar de denne konverteringen.
Gjenfinning/søk	Ja	Søker vil selv ha mulighet til å gjøre innsyn i egen søknad via Nav.no. NAV tilbyr gjenfinning av søknadsdokumenter knyttet til avsender basert på oppslag i metadata.
Sammenstilling	Nei	
Sletting eller tilintetgjøring	Ja	NAV sletter påbegynte søknader etter 14 dager.  NAV sletter sendte søknader etter at de er bekreftet mottatt av kommunale fagsystem.  NAV sletter metadata etter 200 dager.
Utlevering	Nei	

### Kategorier av registrerte

#### Digital søknad om økonomisk sosialhjelp:

- Søker
- Ektefelle
- Barn

#### Innsynsløsning for innbygger:

- Søker
- Ektefelle
- Barn
- Andre (enkeltpersoner eller firma)

#### Innsynsflate for NAV Kontaktsenter:

- Søker
- Andre (enkeltpersoner eller firma)

#### Innsiktsarbeid/målinger

- Innbygger
  - Ansatte i NAV
-

---

## Type personopplysninger

### Digital søknad:

#### Innbygger:

Opplysningstype	Kilde
Personnavn	PDL (Persondataløsningen i NAV)
Folkeregisteridentifikator	PDL
Bostedsadresse Norge	PDL
Bostedskommune	PDL
Oppholdsadresse	PDL
Adressebeskyttelse	PDL
Ansvarlig NAV enhet	NORG
Statsborgerskap	PDL
Telefonnummer	KRR (Kontakt- og reservasjonsregisteret)
Kontonummer	Kontoregister
Sivilstand	PDL
Forelder-barn-relasjon	PDL
Arbeidsforhold	Aa-registeret (Arbeidsgiver- og arbeidstakerregisteret)
Avtalt stillingsprosent	Aa-registeret
Ansettelsesperiode	Aa-registeret
Virksomhet	Aa-registeret
Utbetalinger fra NAV	sokos-utbetaldata for innbygger
Skattbar inntekt	Skatteetaten
Statlig bostøtte	Husbanken

#### Om ektefelle/registrert partner:

Opplysningstype	Kilde
Personnavn	PDL
Folkeregisteridentifikator	PDL
Bostedsadresse Norge	PDL
Bostedskommune	PDL
Oppholdsadresse	PDL
Adressebeskyttelse	PDL

#### Om barn:

Opplysningstype	Kilde
Personnavn	PDL
Folkeregisteridentifikator	PDL
Bostedsadresse Norge	PDL
Bostedskommune	PDL
Oppholdsadresse	PDL
Adressebeskyttelse	PDL
Delt bosted	PDL

#### Metadata:

Opplysningstype	Kilde
Fødselsnummer	Digital søknad
BehandlingsID (egen unik kode pr digitale søknad)	Digital søknad
Søknadstidspunkt	Digital søknad

---

Innsynsløsning for innbygger:

Opplysningstype	Kilde
Personnavn	PDL (Persondataløsningen i NAV)
Folkeregisteridentifikator	PDL
NAV-enhet	Kommunalt fagsystem
Kommune	Kommunalt fagsystem
Stønadstype	Kommunalt fagsystem
Kontonummer	Kommunalt fagsystem
Utbetalingsmottaker	Kommunalt fagsystem
Saksnavn (fritekstfelt)	Kommunalt fagsystem
Etterspurt dokumentasjon (fritekstfelt)	Kommunalt fagsystem
Vedlegg (Filnavn eller innhold)	Innbyggeren
PDF-versjon av innsendt søknad (inneholder da alle søknadsopplysninger nevnt under Digital søknad)	Kommunalt fagsystem

Innsynsflate for NAV Kontaktsenter:

Opplysningstype	Kilde
Personnavn	PDL (Persondataløsningen i NAV)
Folkeregisteridentifikator	PDL
Telefonnummer	KRR (Kontakt- og reservasjonsregisteret)
NAV-enhet	Kommunalt fagsystem
Kommune	Kommunalt fagsystem
Kontonummer	Kommunalt fagsystem
Utbetalingsmottaker	Kommunalt fagsystem
Stønadstype (formål pengene går til)	Kommunalt fagsystem
Saksnavn (fritekstfelt)	Kommunalt fagsystem
Etterspurt dokumentasjon (fritekstfelt)	Kommunalt fagsystem

Innsiktsarbeid/målinger:

Opplysningstype	Kilde
Fornavn	Intervjuobjekt
Epost	Intervjuobjekt
Telefonnummer	Intervjuobjekt
Opplysninger innbygger selv oppgir i intervju eller eventuelle fritekstfelt – Informasjon fra nettleser - hvilke nettsider innbygger har besøkt, nettleser, enhet, operativsystem, tidspunkt, dato, hvor lenge de har vært på siden og cookies.	Intervjuobjekt

---

#### Type særlige kategorier av Personopplysninger

Databehandler skal i utgangspunktet ikke behandle særlige kategorier personopplysninger. Som følge av at løsningen har fritekstfelt, og at innbygger kan laste opp vedlegg, er det en risiko for at behandlingen vil omfatte alle typer særlige kategorier.

#### **Spesifikke sletteregler**

##### Digital søknad om økonomisk sosialhjelp:

NAV sletter data fra søknaden etter 14 dager for påbegynte søknader.

NAV tar vare på metadata i 200 dager for å kunne tilby bedre tjenester til innbyggeren på nav.no.

##### Innsikt/målinger:

Råmateriale fra innsiktsarbeid slettes senest etter 30 dager fra innhenting. Sletting forekommer også etter ønske fra intervjuobjekt og trekking av samtykke.

Samtykke for UX-signals lagres i opptil 30 dager før det slettes, eller mot at intervjuobjektet ber om at data/samtykke skal slettes.

## **15 VEDLEGG 2 TEKNISKE OG ORGANISATORISKE SIKKERHETSTILTAK**

Databehandleren skal som et minimum gjennomføre alle de tiltak som fremkommer av NAVs til enhver tid gjeldende felles retningslinje, utarbeidet av Sikkerhetsseksjonen og IT-avdelingen i NAV, for sikring av tjenester som tilbys behandlingsansvarlig.

Databehandleren kan ikke uten varsling av behandlingsansvarlig gjøre endringer i tiltakene som reduserer graden av datasikkerhet. Databehandleren arbeider kontinuerlig for å forbedre sikkerhetstiltakene i tjenesten og sørger for at de oppdateres i takt med den teknologiske utviklingen.

Data som lagres i, og transporteres til/fra, en tjeneste hos NAVs underdatabehandler krypteres for å sikre at data er utilgjengelig for uvedkommende.

Tilgangsstyringen i tjenesten fra databehandler gir kun personer som har tjenstlig behov tilgang til de data som tilhører den enkelte behandlingsansvarlige. Ansatte hos databehandleren og deres underdatabehandlere gis kun tilgang til data ved tjenstlig behov og styres igjennom NAVs autentiseringsløsning. All tilgang (fra kunden, databehandler eller underdatabehandler) til data, eller til komponenter hvor kundens data blir behandlet, logges og det varsles ved unormaliteter. Tilgangsstyringen i tjenesten, og allerede gitte tilganger, revideres jevnlig.

Alle tjenester produsert av databehandler eller involverte underdatabehandler har høy tilgjengelighet igjennom redundans, backup og velprøvde rutiner for katastrofeberedskap.

---

Alle fysiske lokasjoner hvor databehandler prosesserer og lagrer data i forbindelse med leveranse av tjenesten er sikret med tilgangskontroll, døgnbemannet vakt, kameraovervåkning etc.

Tjenesten og tilhørende rutiner ivaretar tjenestens innbyggere rett til å få innsyn i, rette og slette opplysninger om seg selv innenfor rammene av lovverket. Personopplysninger samlet inn gjennom tilgangsløser og metrikker vil ikke lagres eller behandles lenger enn nødvendig for å oppfylle formålet med behandlingen.

## 16 VEDLEGG 3 GODKJENTE UNDERDATABEHANDLERE

Selskapets navn og org.nr.	Selskapets adresse	Geografisk lokasjon for Behandling (jf. punkt 2.2)	Beskrivelse av hvilken type Behandling	Overføringsgrunnlag
Amplitude	Amplitude Inc. 201 3rd Street, Suite 200 San Francisco, CA 94103 United States	Lagringssted: Frankfurt, Tyskland	Innhente opplysninger om hvilke nettsider som innbygger har besøkt, nettleser, enhet, operativsystem, tidspunkt, dato, hvor lenge de har vært på siden, og cookies.	Personopplysninger behandles ikke utenfor EU/EØS
Task Analytics	Salgskontor Europa: Youngstorget 3 0181 Oslo Norway  Hovedkvarter : 110 Remsen St. Brooklyn Heights New York, NY11201	Lagringssted: Amsterdam, Nederland,  St. Ghislain, Belgia  Supportsted: Dublin, Irland	Verktøy for spørreundersøkelse. Brukes for å undersøke innbyggers opplevelse av nettsider og løsninger på nav.no.  Personopplysninger om innbyggersom behandles: Type nettleser og versjon, Operativsystem, Type enhet (mobil, pc), start og slutt nettside-URL, IP-adresse (lagres ikke sammen med besvarelsen), cookies, besvarelse. Hvis undersøkelsen tillater fritekstfelt, er det risiko for at dette feltet kan inkludere	Personopplysninger behandles ikke utenfor EU/EØS

			personopplysninger oppgitt av innbygger selv.	
GCP	Google Norway AS Bryggegate 6, 0250 Oslo  Hovedkvarter : 1600 Amphitheatre Parkway Mountain View, CA 94043, US	Lagringssted: Google GCP, Hamina, Finland	Svarer til type behandling som beskrevet i denne databehandleravtalen.	Personopplysninger behandles ikke utenfor EU/EØS
UX Signals AS	Postadresse: Kristian Collin Berge, Ringveien 27, 1386 Asker	Lagringsted: EU, Tyskland	Varer og tjenester innen programmering. Benyttes til brukerinnsikt i produktutvikling.  Svarer til type behandling som er beskrevet i denne databehandleravtalen.	Personopplysninger behandles ikke utenfor EU/EØS
UXtweak j.s.a.	Vysoka 26, 81106 Bratislava - Stare Mesto, Slovakia	Lagringssted: EU, Irland	Benyttes til brukerinnsikt.  Svarer til type behandling som er beskrevet i denne databehandleravtalen.	Personopplysninger behandles ikke utenfor EU/EØS