**GDPR-prosjekt**

**Mal for kartlegging av**

**behandling av helse- og personopplysninger**

|  |
| --- |
| **A. LØSNING, PROSESS OG SYSTEM** |
| 1. Navn på løsning, prosess eller system: |
| 2. Dato for etablering av løsning, prosess eller system: |
| 3. Kort og generell beskrivelse av løsning, prosess eller system: |
| OPPLYSNINGER |
| 4. Nevn *alle* typer av helse- og personopplysninger som behandles i beskrevet løsning, prosess eller system: Personopplysninger: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Helseopplysninger: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  |
| BEHANDLINGER |
| 5. Nevn *alle* typer behandling av helse- og personopplysninger som foregår i løsning, prosess eller system:\_\_\_\_ innsamling \_\_\_ sammenstilling\_\_\_\_ utlevering \_\_\_ uttrekk av statistikk, styringsdata mv.\_\_\_\_ lagring \_\_\_ endring av opplysninger \_\_\_\_ tilgjengeliggjøring \_\_\_ retting \_\_\_\_ gi tilgang til \_\_\_ sletting\_\_\_\_ gjenbruk \_\_\_ annen behandling:  |
| 6. Kort beskrivelse av hvordan behandling av helse- og personopplysninger som nevnt i punkt 5 foregår i løsning, prosess eller system (for eksempel til hvem opplysninger er levert, hvem har direkte tilgang til systemene, hvem de samler opplysninger fra?): |
| FORMÅL |
| 7. Formålet med behandlingen av helse- og personopplysninger:Hvis løsning, prosess eller system inneholder flere typer av behandlinger (for eksempel lagring og sammenstilling) som har samme formål, beskriv kun dette formålet:Hvis løsning, prosess eller system inneholder flere typer av behandlinger med ulike formål, beskriv formålet til hver enkelt behandling: |
| HJEMMELSGRUNNLAG |
| 8. Hjemmelsgrunnlag for behandling av helse- og personopplysninger: \_\_\_\_ Forskrift, nevn hjemmel: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_ Lov, nevn hjemmel:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_ Samtykke \_\_\_\_ Avtale, nevn avtale: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_ Annet: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| 9. Er hjemmelsgrunnlaget for behandlingen meldt til personvernombudet/ personvernrådgiver riktig: \_\_\_ Ja. \_\_\_ Nei. Nevn hva som er riktig hjemmelsgrunnlag: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| 10. Finnes det behandling som ikke er meldt til personvernombudet/personvernrådgiver: \_\_\_ Ja. Nevn hvilken behandling: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_ Nei.  |
| **B. ROLLER, ANSVAR OG DATABEHANDLERAVTALER** |
| 1. Direktoratets rolle i behandling av helse- og personopplysninger: \_\_\_\_ Databehandlingsansvarlig, gå til punkt 2  \_\_\_\_ Databehandler, gå til punkt 4 |
| DATABEHANDLINGANSVARLIG |
| 2. Direktoratet er databehandlingsansvarlig. 1. Navn på virksomhet som er databehandler: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
2. Er databehandler avtaleforpliktet til å følge Normen:

\_\_\_ Ja. Hvilken avtale (for eksempel NHN tilknytningsavtale): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Nei1. Kort beskrivelse av hvilket ansvar databehandler har og hvordan de behandler helse- og personopplysninger på vegne av direktoratet:
 |
| 3. Direktoratet er databehandlingsansvarlig sammen med andre (*joint controllers*). 1. Navn på de andre virksomhetene som også er databehandlingsansvarlig: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 b. Er de andre databehandlingsansvarlige avtaleforpliktet til å følge Normen: \_\_\_ Ja. Hvilken avtale (for eksempel NHN tilknytningsavtale): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Nei c. Kort beskrivelse av hvilket ansvar og hvilke oppgaver direktoratet og de andre virksomhetene har:  |
| DATABEHANDLER |
| 4. Direktoratet er databehandler.  a. Navn på virksomhet som er databehandlingsansvarlig: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ b. Er de andre databehandlingsansvarlige avtaleforpliktet til å følge Normen: \_\_\_ Ja. Hvilken avtale (for eksempel NHN tilknytningsavtale): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Nei c. Kort beskrivelse av hvilket ansvar direktoratet har og hvordan direktoratet behandler helse- og personopplysninger på vegne av databehandlingsansvarlig:  |
| 5. Brukes det underleverandør?  \_\_\_\_ Ja. Gå til punkt 6. \_\_\_\_ Nei.  |
| 6. Har databehandlingsansvarlig godkjent underleverandør?  \_\_\_\_ Ja. Navn på underleverandør \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_ Nei.  |
| DATABEHANDLERAVTALE |
| 7. Er det utformet databehandleravtale: \_\_\_\_ Ja. Gå til punkt 6. \_\_\_\_ Nei. Gå til punkt 7. |
| 8. Beskriv hvorvidt databehandleravtale er en egen avtale eller en del av tjenesteavtale: \_\_\_\_ Egen avtale. Dato: \_\_\_\_\_\_\_\_\_\_\_ Parter: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_ En del av tjenesteavtale. Dato: \_\_\_\_\_\_\_\_ Parter: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| 9. Brukes det underleverandør (inkludert virksomheter som direktoratet ikke har databehandleravtale med): \_\_\_\_ Ja, navn på underleverandør: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_ Nei |
| 10. Kort beskrivelse av underleverandørs ansvar, rolle og oppgaver, og hvordan de etter avtalen skal behandle helse- og personopplysninger (hvis relevant):  |
| **C. SAMTYKKE – fylles ut kun når behandling av helse- og personopplysninger er basert på samtykke** |
| 1. Hvordan innhenter dere samtykke fra innbygger? Hvordan kan dere dokumentere i ettertid at samtykke er innhentet? Kort beskrivelse av hvordan samtykke er innhentet og dokumentert: |
| 2. Kort beskrivelse av hvordan samtykke kan trekkes tilbake: |
| 3. Er det gitt informasjon til den registrerte om samtykket:  \_\_\_\_ Ja, beskriv hvilken informasjon som er gitt: \_\_\_\_ Nei. |
| **D. DEN REGISTRERTES RETTIGHETER** |
| 1. *Informasjon*. Kort beskrivelse av all informasjon som gis til den registrerte: |
| 2. *Innsyn.* Kort beskrivelse av hvordan den registrerte kan få innsyn i egne opplysninger: |
| 3. *Retting og sletting.* Kort beskrivelse av hvordan den registrerte kan få rettet og slettet opplysninger: |
| **E. INFORMASJONSSIKKERHET** |
| 1. Kort beskrivelse av hvordan informasjonssikkerhet er ivaretatt med organisatoriske tiltak:  |
| 2. Kort beskrivelse av hvordan informasjonssikkerhet er ivaretatt med tekniske tiltak:  |
| 3. Beskriv hvordan logging skjer og hvordan logging dokumenteres i løsning, system eller prosess: |
| **F. RUTINER** |
| 1. Kort beskrivelse av hvilke skriftlige rutiner som finnes for behandling av helse- og personopplysninger (for eksempel rutiner for retting, sletting, trekk av samtykke osv): |
| 2. Kort beskrivelse av rutiner for internkontroll: |
| 3. Kort beskrivelse av andre rutiner:  |
| 4. Finnes det uformelle/ikke-skriftlige rutiner?  \_\_\_\_ Ja. Kort beskrivelse av uformelle/ikke-skriftlige rutiner: \_\_\_\_ Nei.  |
| **G. OVERFØRING TIL UTLANDET** |
| 1. *Overføring til utlandet.*   Er helse- og personopplysninger overført til utlandet?\_\_\_\_ Ja. Land:  Beskriv ansvar, rolle og oppgaver utenlandske databehandlere har:\_\_\_\_ Nei |
| 2. *Utenlandske databehandlere.*  Er helse- og personopplysninger behandlet av utenlandske virksomheter?\_\_\_\_ Ja. Land:  Beskriv ansvar, rolle og oppgaver de har:\_\_\_\_ Nei |
| **H. VEDLEGG ELLER LINK TIL:** |
| 1. Løsning-, prosess- eller systembeskrivelse
2. Databehandleravtale
3. Samtykkeskjema
4. Informasjon til den registrerte
5. Avtaler
6. Rutiner
7. Annet:
 |
| Utfylt av: |  |

Utfylt dato:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signatur:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(kartleggingsansvarlig)

© Direktoratet for e-helse. Malen er utviklet av GDPR-prosjektet i Direktoratet for e-helse, og kan ikke brukes til kommersielle formål.