RETNINGSLINJER FOR Å BEHANDLE PERSONOPPLYSNINGER OM BRUKERE VED KRISESENTRE

1. Formål

Personopplysninger om brukere ved krisesentrene kan behandles til følgende formål:

- yte bistand til kvinnen og eventuelt hennes barn i krise- og mishandlingssituasjoner
- oppbevare opplysninger for eventuell senere oppfølging

Merknad: Primærformålet er å yte bistand til kvinnen mens hun oppholder seg ved senteret som beboer eller dagbruker. Oppbevaring av opplysninger etter endt opphold for fremtidig oppfølging, for eksempel i forbindelse med bistand i rettssaker, er et nytt formål som fordrer et nytt samtykke. Se personopplysningsloven § 11 bokstav c og punkt 2 nedenfor.

2. Behandlingsgrunnlag

Behandling av opplysninger ved krisesenteret kan bare skje dersom kvinnen har samtykket. Samtykket skal være frivillig, uttrykkelig og informert. Samtykket må også omfatte behandling av opplysninger om eventuelle barn som oppholder seg på senteret.

Unntak fra samtykkekravet kan gjøres dersom senteret har behov for å registrere opplysninger om navn på kvinnen/barn av sikkerhetsmessige årsaker.

Merknad: Behandling av personopplysninger er enhver bruk av personopplysninger, som for eksempel innsamling, registrering, sammenstilling, lagring og utlevering eller en kombinasjon av slike bruksmåter, jf personopplysningsloven § 2 nr 2. En behandling krever hjemmel i personopplysningsloven § 8 og eventuelt § 9.

Samtykke må også innhentes for å behandle opplysninger om barn. Dersom barnets alder og modenhet samt omstendighetene for øvrig tilsier det, kan barnet selv avgi samtykke.

Dersom det behandles opplysninger om far/partner eventuelt andre personer krisesenteret har direkte kontakt med, må også vedkommendes samtykke til behandling av personopplysninger innhentes.

2.1 Utlevering/utveksling av opplysninger

Opplysninger skal utleveres til kommunens barneverntjeneste når det er grunn til å tro at et barn blir mishandlet i hjemmet eller det foreligger andre former for alvorlig omsorgssvikt eller når et barn har vist vedvarende alvorlige adferdsvansker i tråd med Lov om barneverntjenester § 6-4a jf. § 6-4. Kvinnen skal så langt mulig informeres om utleveringen.

Merknad: Det følger av lov om barneverntjenester § 6-4 a med forskrift at medarbeidere ved private krisesentre som får driftskostnadene dekket av det offentlige har opplysningsplikt til barneverntjenesten.

Enhver annen utlevering/utveksling av opplysninger til offentlige institusjoner, etater eller andre krever samtykke.

Merknad: Det er viktig at slikt samtykke konkret dekker den enkelte institusjon/etat eller andre det utveksles opplysninger med.

3. Saklighet/relevans

Det skal kun behandles opplysninger som er saklige og relevante for formålet med oppholdet og eventuell oppfølgingen av beboer. Det skal utvises varsomhet med å behandle opplysninger om tredjeperson.

Merknad: Det gjøres oppmerksom på at tredjeperson vil kunne kreve innsyn i opplysninger som behandles om ham/henne jf personopplysningsloven §§ 18 og 23.

4. Tilgang til opplysningene

I henhold til personopplysningsloven § 13, jf forskriftens § 2-11, skal det foreligge saklig behov for enhver tilgang/innsyn i personopplysninger hvor konfidensialitet er nødvendig. Se også punkt 7.2 nedenfor.

Merknad: Det er daglig leder som autoriserer andres tilgang til opplysningene. Tilgangen skal bygge på en vurdering av det saklige behovet den ansatte har, herunder hvilken funksjon vedkommende har ved senteret. Datatilsynet anbefaler at de ansatte ved senteret skriver under på en taushetserklæring.

5. Oppbevaring av statistikkskjemaer

Skjemaer som er utarbeidet til statistikkformål skal oppbevares adskilt fra øvrige personopplysninger, slik at identifisering ikke er mulig.

Merknad: Statistikkskjemaer for innrapportering til Barne- og familiedepartementet skal være anonyme. Dersom de på en eller annen måte kan kobles til opplysninger om kvinnen, ved løpenummer, navn eller lignende, vil intensjonen om anonymitet ikke være oppfylt.

6. Sletting av personopplysninger

Ved avsluttet opphold skal alle opplysninger om kvinnen/barna slettes/makuleres forsvarlig. Alternativt kan opplysningene utleveres til kvinnen. Dersom kvinnen samtykker til videre oppbevaring, kan opplysningene oppbevares i inntil to år fra tidspunktet for siste kontakt med kvinnen. Lagring av opplysninger utover denne fristen, krever at det innhentes et nytt samtykke.

Dersom kvinnen forlater krisesenteret uten forvarsel, kan opplysninger likevel oppbevares i inntil seks måneder.

7. Sikring av personopplysninger

Datatilsynet gjør spesielt oppmerksom på at alle virksomheter som behandler sensitive personopplysninger må gjennomføre en risikovurdering. Resultatet av risikovurderingen vil gi svar på hvilket risikonivå som er akseptabelt. For hjelp til dette, se Datatilsynets hjemmeside www.datatilsynet.no under menyen "Informasjonssikkerhet", eller ta kontakt med Datatilsynets tilsyns- og sikkerhetsavdeling.

Dersom krisesenteret ikke har egen IT-kompetanse og leier dette inn fra dataforhandlere, må disse gjøres oppmerksom på pliktene databehandler har, jf personopplysningsloven § 15.

Personopplysningene skal som hovedregel behandles i et fysisk isolert datasystem (dvs datasystem uten oppkobling til eksterne nett som for eksempel Internett).

7.1 Fysisk sikring

Det skal treffes tiltak mot uautorisert adgang til utstyr (arbeidsstasjoner, servere og skrivere, samt kopimaskiner og telefaksmaskiner), som brukes for å behandle personopplysninger. Sikkerhetstiltakene skal hindre uautorisert adgang til annet utstyr av betydning for informasjonssikkerheten.

Merknad: Virksomheten skal sørge for at egne lokaler og utstyr er forsvarlig sikret, med spesiell vekt på de rom hvor det er plassert utstyr som benyttes for behandling av sensitive personopplysninger. Den fysiske sikringen av sensitive personopplysninger er en vesentlig del av det totale sikkerhetskonseptet. Trusler som kan utløses ved for dårlig fysisk sikring kan blant annet være:

- *At uvedkommende får tilgang til utstyr hvor sensitive personopplysninger behandles*
- *Tyveri av PC-er eller sikkerhetskopier på dagtid eller ved innbrudd utenom arbeidstiden*
- *Sabotasje eller hærverk mot vitale deler av IT-systemet*

7.2 Sikring av konfidensialitet

Det skal treffes tiltak mot uautorisert innsyn i personopplysninger hvor konfidensialitet er nødvendig. Sikkerhetstiltakene skal også hindre uautorisert innsyn i annen informasjon med betydning for informasjonssikkerheten. Personopplysninger som overføres elektronisk ved hjelp av overføringsmedium utenfor den behandlingsansvarliges fysiske kontroll, skal krypteres eller sikres på annen måte.

Merknad: For lagringsmedium som inneholder personopplysninger skal behovet for sikring av konfidensialitet fremgå ved hjelp av merking eller på annen måte. Dersom lagringsmediet ikke lenger benyttes for behandling av slike opplysninger, skal opplysningene slettes fra lagringsmediet. Tilgang til tjenester og informasjon i nettverk skal kun gis etter tjenstlig behov. Som utgangspunkt skal alle tjenester være sperret. For å kunne begrense tilgang til sensitive personopplysninger legges følgende begrensninger og kontroll med tilgang til informasjon og applikasjonene:

- *Tilgang til alle tjenester og informasjon er i utgangspunktet sperret.*
- *Tilgangskontrollen skal benytte individuelle passord og skal sørge for at brukere kun autoriseres for tilgang til informasjon og tjenester etter tjenstlige behov.*

- *Virksomheten skal angi krav til minimum lengde, sammensetning og varighet av passord.*
- *Virksomheten skal angi krav til maksimalt tillatt tidsrom uten aktivitet fra en bruker før det kreves ny autentisering.*
- *Brukerkonti som ikke har vært benyttet de siste to mnd, alternativt når passord skulle ha vært skiftet, skal sperres.*
- *Det må benyttes et operativsystem eller tredje part sikkerhetsløsning som tilfredsstillende skiller mellom brukeres rettigheter. Dette må skille mellom brukere/brukergruppers (identitet/passord) rettigheter til filsystem/nettverksressurser.*
- *Teknisk sikkerhetsløsning hos bruker skal bidra til å hindre uautorisert utlevering av sensitive personopplysninger ved utilsiktet overføring av data mellom program, eksempelvis ved bruk av "klipp og lim"-funksjon.*
- *Dersom det skal lagres sensitive personopplysninger på bærbar arbeidsstasjon, skal harddisken på disse maskinene krypteres.*

7.3 Tilleggskrav ved tilkobling til eksternt nett

I de tilfeller der krisesenterets nett skal være tilkoblet et eksternt nett (som Internett) må det settes opp sikkerhetsbarrierer (for eksempel to brannmurer).

Merknad: Det vil i den enkelte virksomhet være svært varierende behov for funksjonalitet og derfor ulike sikkerhetsløsninger, uten at det er valgt å dokumentere disse i denne konsesjonen. For eksempel kan brannmurer være unødvendige ved fysisk isolerte nettverk, mens andre løsninger kan bestå av en brannmur og en forsterket ruter.

Funksjonelle krav til sikkerhetsbarriere:

- *Ingen trafikk tillates initiert fra eksterne nettverk og direkte inn på virksomhetens interne nettverk*
- *Tjenester som ikke eksplisitt er tillatt er forbudt*
- *Autentisering av brukere i sikkerhetsbarrieren*
- *Brukerprofil i sikkerhetsbarriere*
- *Det er anbefalt å benytte "Network Address Translation" (NAT) så sikkerhetsbarrieren på denne måten skjuler ressursene på innsiden overfor det eksterne datanettet*
- *Oppdatering av sikkerhetspatcher (hotfix)*
- *Kun bruk av Java med opphav anerkjent av virksomheten (Active X er i utgangspunktet ikke tillat)*
- *Ekstern overføring av sensitive personopplysninger krever kryptering fra sikret sone i en virksomhet til tilsvarende sikret sone hos annen virksomhet*

8. Melding ved opphør av virksomhet

Den behandlingsansvarlige skal ved opphør av virksomheten sende en melding til Datatilsynet med bekreftelse på at personopplysningene er slettet/tilbakeført i samsvar med retningslinjenes pkt 6 og 7.2.