



Deres ref

Vår ref (bes oppgitt ved svar)
GS/-

Dato

KONSESJON TIL Å BEHANDLE PERSONOPPLYSNINGER – PRIVAT BARNEVERNINSTITUSJON

Vi viser til Deres søknad av xx.xx.xxxx om konsesjon til å behandle personopplysninger.

Datatilsynet har vurdert søknaden og gir Dem med hjemmel i personopplysningsloven § 33, jf. § 34, konsesjon til å behandle personopplysninger til følgende formål:
Behandling og oppfølging av beboere ved institusjonen.

Behandlingsansvarlig er øverste leder ved..... Gjennomføringen av det daglige ansvaret kan delegeres.

Konsesjonen er gitt under forutsetning av at behandlingen foretas i henhold til søknaden, de bestemmelser som følger av personopplysningsloven med forskrifter samt vedlagte retningslinjer.

Dersom det skjer endringer i behandlingen i forhold til de opplysninger som er gitt i søknaden, må dette fremmes i ny konsesjonssøknad.

I medhold av personopplysningsloven § 35, fastsettes i tillegg følgende vilkår for behandlingen:

1. Opplysninger om beboer kan behandles uten vedkommendes samtykke jf personopplysningsloven § 9,3.ledd. Behandlingen av personopplysninger bør i størst mulig utstrekning skje i samarbeid med beboer.
2. Den behandlingsansvarlige skal hvert tredje år sende Datatilsynet bekreftelse på at behandlingen skjer i overensstemmelse med søknaden og personopplysningslovens regler.

3. Datatilsynet tar forbehold om at konsesjonen kan bli trukket tilbake eller at nye og endrede vilkår kan bli gitt dersom dette er nødvendig ut fra personvern hensyn.

Med hilsen

Knut-Brede Kaspersen (sign)
avdelingsdirektør

Guro Slettemark
seniorrådgiver

- Vedlegg; Retningslinjer for behandling av personopplysninger i privat barneverninstitusjon



RETNINGSLINJER FOR Å BEHANDLE PERSONOPPLYSNINGER I PRIVAT BARNEVERNINSTITUSJON

1. Behandlingsgrunnlag

I konsesjonen er det fastslått at opplysninger om beboer kan behandles uten vedkommendes samtykke, jf personopplysningsloven § 9, 3. ledd. I den grad beboerens alder og modenhet samt omstendighetene for øvrig tilsier det, bør imidlertid behandlingen av personopplysninger skje i samarbeid med beboer.

Merknad: Hovedregelen er at behandling av sensitive personopplysninger krever den registrertes samtykke jf personopplysningsloven § 9. For den gruppe beboere det her dreier seg om (barn og unge), vil det imidlertid ikke alltid være hensiktsmessig å kreve samtykke. Fravikelse av samtykkekravet bør imidlertid, i den grad beboerens alder og modenhet samt omstendighetene for øvrig tilsier det, kompenseres ved at behandling av personopplysninger skjer med beboerens kunnskap.

2. Saklighet/relevans

Det skal kun behandles opplysninger som er saklige og relevante for formålet med institusjonsoppholdet og den videre oppfølgingen av beboeren. Det skal utvises varsomhet med å samle inn opplysninger om tredjeperson.

Merknad: Fordi innsamling av personopplysninger vanligvis ikke vil være basert på samtykke fra beboer, bør opplysningenes art og omfang begrenses.

Opplysninger som er saklige og relevante for formålet med institusjonsoppholdet og den videre oppfølgingen av beboeren skal imidlertid behandles. Det vises i denne sammenheng til krav om protokollføring og begrunnelse i forskrift om rettigheter og bruk av tvang under opphold i barneverninstitusjon av 12.12 2002.

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

3. Sletting/tilbakeføring av personopplysninger

Ved avsluttet opphold, skal alle personopplysninger gjennomgås. Opplysningene bør, så langt det er mulig og i den grad beboerens alder og modenhet samt omstendighetene for øvrig tilsier det, gjennomgås sammen med beboer. Rapporter, journaler o.l. oversendes barneverntjenesten i kommunen. Opplysninger som ikke lenger er relevante skal slettes/makuleres forsvarlig. Dersom det er sannsynlig at beboer vil vende tilbake til institusjonen, kan oversendelse av rapporter, journaler o.l. utstå i inntil ett år.

Ved avvikling av driften (konkurs, nedleggelse o.l.) skal alle personopplysninger om beboere overføres til barneverntjenesten eller til Barne,- ungdoms, og familieetaten.

4. Lagring av basisopplysninger

Etter beboers/verges samtykke, kan basisopplysninger som navn, fødselsdato adresse og oppholdets varighet oppbevares uavhengig av retningslinjenes pkt. 3.

5. 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 tilsyn- og sikkerhetsavdeling.

Dersom institusjonen 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 f.eks Internett).

5.1 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. 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 bl.a. 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

5.2 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. 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
- Sperring av brukerkonti som ikke har vært benyttet de siste to mnd, alternativt når passord skulle ha vært skiftet
- Det må benyttes et operativsystem eller tredje part sikkerhetsløsning som tilfredsstillende skiller mellom brukeres rettigheter. Dette må skille mellom brukere/brukergrupper (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

5.3 Tilleggskrav ved tilkobling til eksternt nett

I de tilfeller der institusjonens nett skal være tilkoblet et eksternt nett (som Internett) må det settes opp sikkerhetsbarrierer (for eksempel to brannmurer). Det vil i den enkelte virksomhet være svært varierende behov for funksjonalitet og derfor ulike sikkerhetsløsninger, uten at det er valgt å dokumentere disse her. 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 tillatt)
- Ekstern overføring av sensitive personopplysninger krever kryptering fra sikret sone i en virksomhet til tilsvarende sikret sone hos annen virksomhet

6. 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 3 og 5.2.