Ketil Øyesvold Melhus
Registrert Gestaltterapeut MNGF

DOKUMENTASJON AV PERSONVERN

Dette dokumentet beskriver hvordan Ketil Øyesvold Melhus oppfyller kravene i personopplysningsloven og EUs personvernforordning, GDPR.

Versjon 1
04.12.2018

Innhold

1 Om virksomheten

Ketil Øyesvold Melhus er en privatpraktiserende gestaltterapeut, medlem av Norsk Gestaltterapeut Forening (NGF) og registrert i Register for Alternativ Behandling. Virksomheten tilbyr individualterapi, terapi for par og grupper. Virksomheten er behandlingsansvarlig for sine Klienter, kunder og leverandører. Virksomheten er ikke databehandler.

Generelt lagrer virksomheten få personopplysninger. For hver rullerende 5-årsperiode lagres det opplysninger om ca. 50 personer. Det lagres kun alminnelig kontaktinformasjon og ordinære regnskapsopplysninger. I tillegg kommer journaler, men disse er anonymisert og kryptert. Lagring av helseopplysninger er også regulert av Lov om alternativ behandling av sykdom mv. og NGFs etiske retningslinjer.

Kontakt og fakturainformasjon lagres i elektronisk journalsystem, passordbeskyttet og kryptert, og i elektronisk regnskapssystem. Det lagres ingen personopplysninger på papir.

Virksomheten benytter to eksterne databehandlere, Domeneshop og Tripletex. Systemene krever pålogging og kommunikasjonen over internett er kryptert. Det lagres ikke sensitive opplysninger. Ut over allmenn kontaktinformasjon sendes det ingen personopplysninger ukryptert per epost.

2 Personvernansvarlig

Siden virksomheten behandler få personopplysninger om et lite antall personer har virksomheten valgt å ikke ha et personvernombud. Ketil Øyesvold Melhus er ansvarlig for personvern i virksomheten.

3 Vurdering av risiko for personers rettigheter

Protokollen, se kapittel 5, viser at virksomheten har kontroll på sine behandlinger og at personopplysninger behandles og lagres forsvarlig.

Det vurderes at sannsynligheten for at personopplysninger skal komme på avveie, ødelegges eller slettes er lav og at konsekvensen i så fall ville vært liten.

Basert på dette mener virksomheten at behandling av personopplysninger utføres slik at det er lav risiko for brudd på enkeltpersoners rettigheter og at det ikke er nødvendig med ytterligere konsekvensutredning.

4 Personvernerklæring

Virksomhetens personvernerklæring i henhold til artikkel 12 finnes i dokumentet «Personvern - Personvernerklæring - Ketil Øyesvold Melhus MNGF.pdf». Personvernerklæringen brukes som vedlegg til klientavtalen og er tilgjengelig på virksomhetens WEB-side https://www.gestaltterapi.me.

5 Kartlegging av behandling

5.1 Protokoll

En oversikt over behandlingsaktiviteter i henhold til artikkel 30 finnes i dokumentet "Personvern - Oversikt over personopplysninger som behandles - Ketil Øyesvold Melhus MNGF.pdf".

5.2 Rutinebeskrivelser

5.2.1 Ny klient

Når en potensiell ny klient tar kontakt avtales det et første møte. Om møtet fører til at det inngås en avtale så lagres den signerte avtalen kryptert og kontaktopplysninger registreres i Tripletex.

5.2.2 Journalføring

Det føres journal etter hver konsultasjon. Journalen lagres passordbeskyttet (128bit AES) på Microsoft Onedrive, passordbeskyttet og kryptert.

5.2.3 Fakturering og oppfølging

Kunden belastes via iZettle terminal. I etterkant opprettes kunden i Tripletex med fornavn. Faktura sendes ikke til kunden.

5.2.4 Innsyn

De registrerte har rett til innsyn i egne personopplysninger. Følgende prosedyre skal følges:

Akt. Nr.	Hvem	Aktivitet	Hvordan
1.	Den registrerte	Send krav om innsyn.	Per epost eller brev.
2.	Terapeut	Eventuelt: Bekreft mottak og informer om tidsfrist (30 dager).	Per epost.
3.	Terapeut	Hent personopplysninger fra Excel-journal	Excel
4.	Terapeut	Søk etter den registrerte i epostarkivet.	Gmail
5.	Terapeut	Søk etter den registrerte i filarkivet.	Excel
6.	Terapeut	Legg alt, pluss dokumentet " Personvern - Oversikt over personopplysninger som behandles", i et ZIP-arkiv som passordbeskyttes.	Gmail
7.	Terapeut	Send ZIP-fil til den registrerte per epost.	Gmail
8.	Terapeut	Send passord til den registrerte per SMS.	iPhone
9.	Terapeut	Slett ZIP-fil etter <nn> dager.	Gmail/Onedrive

5.2.5 Korrigering

De registrerte har rett til å få korrigert egne personopplysninger. Følgende prosedyre skal følges:

Akt. Nr.	Hvem	Aktivitet	Hvordan

1.	Den registrerte	Send krav om korrigering.	Per epost eller brev.
2.	Terapeut	Eventuelt: Bekreft mottak og informer om tidsfrist (30 dager).	Per epost.
3.	Terapeut	Korriger personopplysninger i Word	Opprette nytt korrigert dokument og lagre passordbeskyttet/kryptert
4.	Terapeut	Bekreft korrigering.	Per epost.

5.2.6 Retten til begrensning

Dette vil være det samme som å avslutte avtaleforholdet og anses som ikke relevant.

5.2.7 Retten til å motsette seg behandling

Virksomheten har ikke behandlinger hvor det er aktuelt å motsette seg behandling.

5.2.8 Overføring av sine personopplysninger (Dataportabilitet)

Virksomheten anser kravet til dataportabilitet å være dekket gjennom rutinen for innsyn.

5.2.9 Retten til å bli glemt

De registrerte har rett til å "bli glemt", dvs å avslutte avtaleforholdet og få personopplysninger slettet. Følgende prosedyre skal følges:

Akt. Nr.	Hvem	Aktivitet	Hvordan
1.	Den registrerte	Send krav om å "bli glemt".	Per epost eller brev.
2.	Terapeut	Eventuelt: Bekreft mottak og informer om tidsfrist (30 dager).	Per epost.
3.	Terapeut	Slett personopplysninger i OneDrive. Kan gjøres ved å anonymisere eller pseudonymisere "kundekortet".	Manuelt i Word/Onedrive
4.	Terapeut	Søk etter den registrerte i epostarkivet og slett all epost. <husk at det er lov til å ta vare på epost som kan tenkes å være nødvendig for å håndtere en reklamasjon eller forsvare et rettskrav>	Manuelt i epostsystemet.
5.	Terapeut	Søk etter den registrerte i filarkivet og slett, anonymiser eller pseudonymiser alle dokumenter. <husk at det er lov til å ta vare på dokumenter som kan tenkes å være nødvendig for å håndtere en reklamasjon eller forsvare et rettskrav>	Word/OneDrive
6.	Terapeut	Bekreft at avtaleforholdet er avsluttet.	Per epost eller brev.

6 Databehandlere

Virksomheten bruker følgende eksterne databehandlere:

6.1 Domeneshop

Domeneshop leverer Eposttjenester og WEB-hotell for Virksomhetens WEB-sider. Domeneshop har ingen separat databehandleravtale men har alle krav til dokumentasjon i henhold til GDPR i sin generelle avtale.

6.2 Tripletex

Tripletex utfører alle økonomi og regnskapstjenester for virksomheten.

7 Arkivering

Klientavtaler og journaler lagres på separate OneDrive-konti. SMS lagres på iPhone. Epost lagres i Gmail

8 Informasjonssikkerhet

8.1 Konfidensialitet

Virksomhetens eget datautstyr og alle eksterne systemer er passordbeskyttet for å hindre uvedkommende i å få tilgang til personopplysninger og annet. Kommunikasjon over internett er kryptert. Trådløse nett på arbeidssted og hjemmekontor er lukket og passordbeskyttet.

8.2 Integritet

Det er kun Ketil Øyesvold Melhus som har tilgang til å registrere, endre og slette personopplysninger i egne systemer. Alle databehandlere oppdaterer personopplysninger kun etter instruks fra Ketil Øyesvold Melhus. Alle databehandlere har rutiner for sikkerhetskopiering og gjenoppretting av data.

8.3 Tilgjengelighet.

Det lagres ikke personopplysninger lokalt på virksomhetens datautstyr. Alle databehandlere har reservesystemer tilgjengelig i tilfelle det skulle oppstå problemer med tilgang til hovedsystemene.

9 Innebygd personvern

Virksomheten har ingen egenutviklede systemer og tilbyr ingen systemer til andre.

10 Varsling av avvik

Om det skal varsles eller ikke avhenger av risikoen ved avviket. Virksomheten må selv vurdere om det er sannsynlig at avviket vil medføre ingen risiko, lav risiko, middels risiko eller høy risiko for brudd på personvernet til de berørte.

Hvis vurderingen viser at det er ingen eller lav risiko er det ikke nødvendig å varsle, men avviket skal uansett dokumenteres i henhold til rutinen nedenfor.

10.1 Varsling til Datatilsynet

Hvis vurderingen viser at avviket sannsynligvis medfører middels eller høy risiko skal det varsles til Datatilsynet, innen 72 timer etter at avviket ble oppdaget, via skjema i Altinn: https://www.altinn.no/skjemaoversikt/datatilsynet/melding-om-avvik-datatilsynet/

10.2 Varsling til de berørte

Varsling til de berørte skal skje når det er sannsynlig at avviket vil medføre en høy risiko for brudd på personvernet til de berørte. Varsling til de berørte skal skje så snart som mulig ved å bruke skjema i dokumentet "Personvern - Varsling til de berørte ved avvik – Ketil Øyesvold Melhus.docx ".

10.3 Rutine for avvikshåndtering

Følgende prosedyre skal følges:

Akt. Nr.	**Hvem**	**Aktivitet**	**Hvordan**
1.	Den som oppdager eller informeres om avviket.	Informer personvernansvarlig (PVA) og styret så raskt som mulig.	Per telefon eller epost.
2.	PVA	Start avvikshåndtering.	
3.	PVA	Lag en liste over hvem som er berørt.	
4.	PVA	Kartlegg mulige konsekvenser.	
5.	PVA	Kartlegg mulige tiltak og iverksett umiddelbart om mulig.	
6.	PVA	Vurder om det er sannsynlig at avviket vil medføre en middels eller høy risiko for personvernet til de berørte.	
Hvis ja, starte varsling:			
7.	PVA	Fyll ut varslingsskjema til Datatilsynet på Altinn.	
8.	PVA	Vurder om det er sannsynlig at avviket vil medføre en høy risiko for personvernet til de berørte.	
Hvis ja, varsle til de berørte:			
9.	PVA	Fyll ut skjema til de berørte.	
10.	PVA	Send skjemaet per epost til de berørte på listen.	
Og uansett:			
11.	PVA	Iverksett eventuelle ytterligere tiltak.	
12.	PVA	Evaluer om iverksatte tiltak har lukket avviket.	
13.	PVA	Dokumenter avviket, avviksbehandlingen og eventuelle tiltak for den årlige revisjonen.	

11 Internkontroll

Virksomheten har ikke behov for et omfattende internkontrollsystem. I tillegg til avviksprosedyren dokumentert over finnes det et egenkontrollskjema, dokumentet "Personvern - Årlig egenkontroll - 2019 – Ketil Øyesvold Melhus.docx", og en prosedyre for årlig revisjon, se nedenfor.

11.1 Årlig revisjon

Virksomheten skal en gang i året, basert på egenkontrollskjemaet, gjøre følgende:

1. Revidere all dokumentasjon av personvern og vurdere om det er behov for endringer.
2. Dokumentere og gjennomføre eventuelle endringer.
3. Gå gjennom egenkontrollskjemaet og vurdere om det er behov for endringer.
4. Dokumentere og gjennomføre eventuelle endringer.
5. Revidere eventuelle avvik siste år.
6. Slette historikk det ikke lenger er grunnlag for å beholde.
7. Signere og arkivere egenkontrollskjemaet.