

Hege Jensen ENK
Registrert Gestaltherapeut student MNGF

DOKUMENTASJON
AV
PERSONVERN

Dette dokumentet beskriver hvordan Hege Jensen ENK oppfyller kravene i personopplysningsloven og EUs personvernforordning, GDPR.

Versjon 1
01.11.2021

Innhold

1	Om virksomheten.....	3
2	Personvernansvarlig.....	3
3	Vurdering av risiko for personers rettigheter.....	3
4	Personvernerklæring.....	3
5	Kartlegging av behandling.....	4
5.1	Protokoll.....	4
5.2	Rutinebeskrivelser.....	4
5.2.1	Ny klient.....	4
5.2.2	Journalføring.....	4
5.2.3	Fakturering og oppfølging.....	4
5.2.4	Innsyn.....	4
5.2.5	Korrigerings.....	4
5.2.6	Retten til begrensning.....	5
5.2.7	Retten til å motsette seg behandling.....	5
5.2.8	Overføring av sine personopplysninger (Dataportabilitet).....	5
5.2.9	Retten til å bli glemt.....	5
6	Databehandlere.....	5
6.1	Domeneshop.....	5
6.2	Økonomi og regnskap.....	6
6.3	Journalssystem.....	6
6.4	Eventuelt flere.....	Feil! Bokmerke er ikke definert.
7	Arkivering.....	6
8	Informasjonssikkerhet.....	6
8.1	Konfidensialitet.....	6
8.2	Integritet.....	6
8.3	Tilgjengelighet.....	6
9	Innebygd personvern.....	6
10	Varsling av avvik.....	6
10.1	Varsling til Datatilsynet.....	6
10.2	Varsling til de berørte.....	6
10.3	Rutine for avvikshåndtering.....	7
11	Internkontroll.....	8
11.1	Årlig revisjon.....	8

1 Om virksomheten

Hege Jensen ENK er en privatpraktiserende gestaltterapeutstudent, medlem av Norsk Gestaltterapeut Forening (NGF) og registrert i Register for Alternativ Behandling. Virksomheten tilbyr individualterapi, kurs, samtaler og terapi for par.

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. 100 personer. Det lagres kun alminnelig kontaktinformasjon og ordinære regnskapsopplysninger. I tillegg kommer journaler, men disse er anonymisert. Lagring av helseopplysninger er også regulert av Lov om alternativ behandling av sykdom mv. og NGF sine etiske retningslinjer.

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

Virksomheten benytter tre eksterne databehandlere, web-hotell, journalsystem og regnskapssystem. 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. Hege Jensen 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 – Hege Jensen ENK.pdf». Personvernerklæringen er tilgjengelig på virksomhetens WEB-sider. hegejensen.no

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 – Hege Jensen ENK.pdf".

5.2 Rutinebeskrivelser

5.2.1 Ny klient

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

5.2.2 Journalføring

Det føres journal på PC i et enkelt internt journalsystem etter hver konsultasjon.

5.2.3 Fakturering og oppfølging

Klienten betaler med Vips.

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 <systemet>.	<fyll ut> <eksport til Excel?>
4.	Terapeut	Søk etter den registrerte i epostarkivet.	<fyll ut>
5.	Terapeut	Søk etter den registrerte i filarkivet.	<fyll ut>
6.	Terapeut	Legg alt, pluss dokumentet " Personvern - Oversikt over personopplysninger som behandles", i et ZIP-arkiv som passordbeskyttes.	<fyll ut>
7.	Terapeut	Send ZIP-fil til den registrerte per epost.	<fyll ut>
8.	Terapeut	Send passord til den registrerte per SMS.	<fyll ut>
9.	Terapeut	Slett ZIP-fil etter <30> dager.	<fyll ut>

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	Korrigerer personopplysninger i <systemet>.	
4.	Terapeut	Bekreft korrigerings.	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 systemet. Kan gjøres ved å anonymisere eller pseudonymisere "kundekortet".	Manuelt
4.	Terapeut	Søk etter den registrerte i epostarkivet og slett all epost. 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. Det er lov til å ta vare på dokumenter som kan tenkes å være nødvendig for å håndtere en reklamasjon eller forsvare et rettskrav.	Manuelt.
6.	Terapeut	Bekreft at avtaleforholdet er avsluttet.	Per epost eller brev.

6 Databehandlere

Virksomheten per dags dato bruker ingen 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 Økonomi og regnskap

Hege Jensen ENK utfører alle økonomi og regnskapstjenester for virksomheten.

6.3 Journalsystem

Diagnosesystem utarbeidet av Dann Van Baalen.

7 Arkivering

Dokumenter, epost og annet arkiveres kun digitalt på egnet PC.

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 passord beskyttet.

8.2 Integritet

Det er kun Hege Jensen som har tilgang til å registrere, endre og slette personopplysninger i egne systemer. Alle databehandlere oppdaterer personopplysninger kun etter instruks fra Hege Jensen. Alle dokumenter med personopplysninger oppbevares i låst brannsikkert arkivskap og er beskyttet mot skader og ødeleggelse.

8.3 Tilgjengelighet.

Det lagres ikke personopplysninger lokalt på virksomhetens datautstyr. Virksomheten har ingen egenutviklede systemer og tilbyr ingen systemer til andre.

9 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.

9.1 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/>

9.2 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 skjemaet i dokumentet "Personvern - Varsling til de berørte ved avvik – Hege Jensen ENK.docx".

9.3 Rutine for avvikshåndtering

Følgende prosedyre skal følges:

Akt. Nr.	Hvem	Aktivitet	Hvordan
1.	Den som oppdager eller informeres om avviket.	Informer personvernansvarlig (PVA) så raskt som mulig.	Per telefon. Tilgjengelig dokumentasjon sendes per epost.
2.	PVA	Beskriv omfanget.	Lag en liste over hvor mange: 1. Personer som er eksponert. 2. Personer eller virksomheter som har mottatt opplysningene. Listen skal inneholde kontaktopplysninger, minst navn og enten epostadresse eller telefonnummer.
3.	PVA	Kartlegg mulige konsekvenser.	Basert på omfang og det aktuelle avviket, lag liste over mulige konsekvenser.
4.	PVA	Kartlegg mulige tiltak.	Basert på mulige konsekvenser lages liste over tiltak.
5.	PVA	Iverksett tiltak umiddelbart hvis nødvendig.	Avhengig av situasjonen.
6.	PVA	Vurder om det er sannsynlig at avviket vil medføre en middels eller høy risiko for personvernet til de berørte.	Basert på omfang, konsekvens og sannsynlighet, vurderes risiko.
Hvis ja, start varsling:			
7.	PVA	Fyll ut varslings skjema til Datatilsynet på Altim .	Via web-leser.
8.	PVA	Er det sannsynlig at avviket vil medføre en høy risiko for personvernet til de berørte?	Basert på risikovurderingen i punkt 6.
Hvis ja, varsle til de berørte:			
9.	PVA	Fyll ut skjema til de berørte.	Bruk skjema i dokumentet "Varsling til de berørte ved avvik".
10.	PVA	Send skjemaet til de berørte på listen.	Manuelt per epost.
Og uansett:			

11.	PVA	Vurder eventuelle ytterligere tiltak.	Avhengig av situasjonen.
12.	PVA	Evaluer om iverksatte tiltak har lukket avviket.	Vurder om tiltakene var gode nok. Hvis ikke, gå til punkt 11.
13.	PVA	Dokumenter avviket, avviksbehandlingen og eventuelle tiltak for den årlige revisjonen.	Dokumenter avviksbehandlingen og eventuelle tiltak i et eget dokument, som lagres sammen med avviksskjemaet i egen mappe.

10 Internkontroll

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

10.1 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.