**<eventuelt logo>**

**<firmanavn>**

**Registrert Gestaltterapeut MNGF**

**DOKUMENTASJON**

**AV**

**PERSONVERN**

Dette dokumentet beskriver hvordan <firmanavn> oppfyller kravene i personopplysningsloven og EUs personvernforordning, GDPR.

**Versjon 1**

**dd.mm.2018**

**Innhold**

[1 Om virksomheten 3](#_Toc526084894)

[2 Personvernansvarlig 3](#_Toc526084895)

[3 Vurdering av risiko for personers rettigheter 3](#_Toc526084896)

[4 Personvernerklæring 4](#_Toc526084897)

[5 Kartlegging av behandling 4](#_Toc526084898)

[5.1 Protokoll 4](#_Toc526084899)

[5.2 Rutinebeskrivelser 4](#_Toc526084900)

[5.2.1 Ny klient 4](#_Toc526084901)

[5.2.2 Journalføring 4](#_Toc526084902)

[5.2.3 Fakturering og oppfølging 4](#_Toc526084903)

[5.2.4 Innsyn 4](#_Toc526084904)

[5.2.5 Korrigering 5](#_Toc526084905)

[5.2.6 Retten til begrensning 5](#_Toc526084906)

[5.2.7 Retten til å motsette seg behandling 5](#_Toc526084907)

[5.2.8 Overføring av sine personopplysninger (Dataportabilitet) 5](#_Toc526084908)

[5.2.9 Retten til å bli glemt 5](#_Toc526084909)

[6 Databehandlere 6](#_Toc526084910)

[6.1 Domeneshop 6](#_Toc526084911)

[6.2 <økonomi og regnskap> 6](#_Toc526084912)

[6.3 <journalsystem> 6](#_Toc526084913)

[6.4 <eventuelt flere> 6](#_Toc526084914)

[7 Arkivering 6](#_Toc526084915)

[8 Informasjonssikkerhet 7](#_Toc526084916)

[8.1 Konfidensialitet 7](#_Toc526084917)

[8.2 Integritet 7](#_Toc526084918)

[8.3 Tilgjengelighet. 7](#_Toc526084919)

[9 Innebygd personvern 7](#_Toc526084920)

[10 Varsling av avvik 7](#_Toc526084921)

[10.1 Varsling til Datatilsynet 7](#_Toc526084922)

[10.2 Varsling til de berørte 8](#_Toc526084923)

[10.3 Rutine for avvikshåndtering 8](#_Toc526084924)

[11 Internkontroll 9](#_Toc526084925)

[11.1 Årlig revisjon 9](#_Toc526084926)

# Om virksomheten

<personnavn> er en privatpraktiserende gestaltterapeut, medlem av Norsk Gestaltterapeut Forening (NGF) og registrert i Register for Alternativ Behandling. Virksomheten tilbyr <fyll ut det som passer, for eksempel individualterapi, terapi for par og grupper, veiledning og undervisning av studenter ved Norsk Gestaltinstitutt (NGI), veiledning av gestaltterapeuter og annen veiledning>. <beskriv eventuell annen tilleggsvirksomhet>

Virksomheten er behandlingsansvarlig for sine Klienter, kunder og leverandører <legg til eventuelle andre>. Virksomheten er ikke databehandler.

Vurder teksten i dette avsnittet og tilpass til din egen virksomhet

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

Beskriv kort hvordan du håndterer journal, du kan detaljere lenger ned i dette dokumentet,

for eksempel:

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

Eller:

<Kontakt og fakturainformasjon lagres på klientskjema på papir i klientmappen sammen med journal på papir og andre klientdokumenter. Skriv også kort om fakturering og regnskap>

Kort om eventuelle databehandlere og informasjonssikkerhet, for eksempel:

<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.>

Eller, i den andre ytterligheten:

<Virksomheten benytter ingen eksterne databehandlere. Klientmapper og andre dokumenter lagres i låsbart brannsikkert arkivskap.>

# Personvernansvarlig

Siden virksomheten behandler få personopplysninger om et lite antall personer har virksomheten valgt å ikke ha et personvernombud. <navn> er ansvarlig for personvern i virksomheten.

# 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.

# Personvernerklæring

Juster avhengig av om du er rent papirbasert eller ikke:

Virksomhetens personvernerklæring i henhold til artikkel 12 finnes i dokumentet «Personvern - Personvernerklæring - <firmanavn>.pdf». Personvernerklæringen brukes som vedlegg til klientavtalen< og er tilgjengelig på virksomhetens WEB-sider>.

# Kartlegging av behandling

## Protokoll

En oversikt over behandlingsaktiviteter i henhold til artikkel 30 finnes i dokumentet "Personvern - Oversikt over personopplysninger som behandles - <firmanavn>.pdf".

## Rutinebeskrivelser

### Ny klient

<Når en potensiell ny klient tar kontakt avtales det et første møte. Om møtet fører til at det inngås en avtale så>

For eksempel:

<lagres den signerte avtalen og kontaktopplysninger registreres i journalsystemet.>

Eller:

<lagres den signerte avtalen og kontaktopplysninger i en ny klientmappe i arkivskapet.>

### Journalføring

<Det føres journal i journalsystemet etter hver konsultasjon.>

<Om du ikke har et eksternt journalsystem, men bruke dokumenter på PC eller MAC eller har en papirbasert journal så beskriv dette i mer detalj her>

### Fakturering og oppfølging

Kunden faktureres etter avtale ved at faktura opprettes og sendes fra journalsystemet.

### Innsyn

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

Denne rutinen må tilpasses i henhold til hva slags systemer man bruker og om man for eksempel er helt papirbasert.

For eksempel:

|  |  |  |  |
| --- | --- | --- | --- |
| Akt. Nr. | Hvem | Aktivitet | Hvordan |
|  | Den registrerte | Send krav om innsyn. | Per epost eller brev. |
|  | Terapeut | Eventuelt: Bekreft mottak og informer om tidsfrist (30 dager). | Per epost. |
|  | Terapeut | Hent personopplysninger fra <systemet>. | <fyll ut><eksport til Excel?> |
|  | Terapeut | Søk etter den registrerte i epostarkivet. | <fyll ut> |
|  | Terapeut | Søk etter den registrerte i filarkivet. | <fyll ut> |
|  | Terapeut | Legg alt, pluss dokumentet " Personvern - Oversikt over personopplysninger som behandles", i et ZIP-arkiv som passordbeskyttes. | <fyll ut> |
|  | Terapeut | Send ZIP-fil til den registrerte per epost. | <fyll ut> |
|  | Terapeut | Send passord til den registrerte per SMS. | <fyll ut> |
|  | Terapeut | Slett ZIP-fil etter <nn> dager. | <fyll ut> |

### Korrigering

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

Denne rutinen må tilpasses i henhold til hva slags systemer man bruker og om man for eksempel er helt papirbasert.

For eksempel:

|  |  |  |  |
| --- | --- | --- | --- |
| Akt. Nr. | Hvem | Aktivitet | Hvordan |
|  | Den registrerte | Send krav om korrigering.  | Per epost eller brev. |
|  | Terapeut | Eventuelt: Bekreft mottak og informer om tidsfrist (30 dager). | Per epost. |
|  | Terapeut | Korriger personopplysninger i <systemet>. | <fyll ut> |
|  | Terapeut | Bekreft korrigering. | Per epost. |

### Retten til begrensning

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

### Retten til å motsette seg behandling

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

### Overføring av sine personopplysninger (Dataportabilitet)

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

### 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:

Denne rutinen må tilpasses i henhold til hva slags systemer man bruker og om man for eksempel er helt papirbasert.

For eksempel:

|  |  |  |  |
| --- | --- | --- | --- |
| Akt. Nr. | Hvem | Aktivitet | Hvordan |
|  | Den registrerte | Send krav om å "bli glemt".  | Per epost eller brev. |
|  | Terapeut | Eventuelt: Bekreft mottak og informer om tidsfrist (30 dager). | Per epost. |
|  | Terapeut | Slett personopplysninger i <systemet>. Kan gjøres ved å anonymisere eller pseudonymisere "kundekortet". | Manuelt i <systemet>. |
|  | 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. |
|  | 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> | <fyll ut> |
|  | Terapeut | Bekreft at avtaleforholdet er avsluttet. | Per epost eller brev. |

# Databehandlere

Juster nedenfor i henhold til din virksomhet:

Enten:

<Virksomheten bruker ingen eksterne databehandlere:>

Eller:

<Virksomheten bruker følgende eksterne databehandlere:>

## 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.

## <økonomi og regnskap>

<økonomi og regnskap> utfører alle økonomi og regnskapstjenester for virksomheten. Osv, osv.>

## <journalsystem>

<beskriv>

## <eventuelt flere>

<beskriv>

# Arkivering

<beskrivelse av hvordan dokumenter, epost og annet arkiveres>

# Informasjonssikkerhet

Eksemplet nedenfor er basert på at du har eksterne databehandlere til journal, fakturering, økonomi og regnskap, at du har eget datautstyr men at du ikke lagrer (identifiserbare) personopplysninger på eget utstyr. Du må tilpasse slik at det passer din egen virksomhet:

## 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.>

Om du er helt papirbasert kan det for eksempel stå:

<Alle dokumenter med personopplysninger oppbevares i låst arkivskap og er ikke tilgjengelig for uvedkommende.>

## Integritet

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

Om du er helt papirbasert kan det for eksempel stå:

<Alle dokumenter med personopplysninger oppbevares i låst brannsikkert arkivskap og er beskyttet mot skader og ødeleggelser.>

## Tilgjengelighet.

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

Om du er helt papirbasert kan det for eksempel stå:

<Alle dokumenter med personopplysninger er lett tilgjengelig ved behov.>

# Innebygd personvern

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

# 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.

Bruk gjerne skjemaet i dokumentet "Personvern - Varsling til de berørte ved avvik - <firma>.docx " til å dokumentere avviket, selv om risikovurderingen tilsier at det ikke er nødvendig å varsle de berørte.

## 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/>

## 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 - <firma>.docx ".

## Rutine for avvikshåndtering

Følgende prosedyre skal følges:

Denne rutinen må tilpasses i henhold til hva slags systemer man bruker og om man for eksempel er helt papirbasert.

For eksempel:

|  |  |  |  |
| --- | --- | --- | --- |
| **Akt. Nr.** | **Hvem** | **Aktivitet** | **Hvordan** |
|  | Den som oppdager eller informeres om avviket. | Informer personvernansvarlig (PVA) så raskt som mulig. | Per telefon.Tilgjengelig dokumentasjon sendes per epost. |
|  | 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. |
|  | PVA | Kartlegg mulige konsekvenser. | Basert på omfang og det aktuelle avviket, lag liste over mulige konsekvenser.  |
|  | PVA | Kartlegg mulige tiltak. | Basert på mulige konsekvenser lages liste over tiltak. |
|  | PVA | Iverksett tiltak umiddelbart hvis nødvendig. | Avhengig av situasjonen. |
|  | 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: |
|  | PVA | Fyll ut varslingsskjema til Datatilsynet på [Altinn](https://www.altinn.no/skjemaoversikt/datatilsynet/melding-om-avvik-datatilsynet/). | Via web-leser. |
|  | 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: |
|  | PVA | Fyll ut skjema til de berørte. | Bruk skjema i dokumentet "Varsling til de berørte ved avvik". |
|  | PVA | Send skjemaet til de berørte på listen. | Manuelt per epost. |
| Og uansett: |
|  | PVA | Vurder eventuelle ytterligere tiltak. | Avhengig av situasjonen. |
|  | PVA | Evaluer om iverksatte tiltak har lukket avviket. | Vurder om tiltakene var gode nok. Hvis ikke, gå til punkt 11. |
|  | 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 mappen "Avvik - <år>" |

# Internkontroll

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

## 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.