



Bjørn Gunaketu Kjønstad - Pustepause

Registrert Gestaltterapeut MNGF

**DOKUMENTASJON
AV
PERSONVERN**

Dette dokumentet beskriver hvordan Pustepause oppfyller kravene i personopplysningsloven og EUs personvernforordning, GDPR.

**Versjon 1.2
17.10.182018**

Innhold

1	Om virksomheten.....	3
2	Personvernansvarlig.....	3
3	Vurdering av risiko for personers rettigheter.....	3
4	Personvernerklæring.....	4
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.....	5
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.....	6
6.1	Domeneshop.....	6
6.2	WIX.....	6
6.3	Conta Faktura og Microsoft Excel.....	6
6.4	Microsoft OneNote journalsystem>.....	6
7	Arkivering.....	6
8	Informasjonssikkerhet.....	6
8.1	Konfidensialitet.....	6
8.2	Integritet.....	6
8.3	Tilgjengelighet.....	7
9	Innebygd personvern.....	7
10	Varsling av avvik.....	7
10.1	Datatilsynet.....	7
10.2	De berørte.....	7
10.3	Rutine for avvikshåndtering.....	7
11	Internkontroll.....	8
11.1	Årlig revisjon.....	8

1 Om virksomheten

Bjørn Gunaketu Kjønstad 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, veiledning, leder- og teamutvikling, mindfulnessundervisning.

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. 150 personer. Det lagres kun alminnelig kontaktinformasjon og ordinære regnskapsopplysninger. I tillegg kommer journaler, men disse er anonymisert og lagret kryptert med passord. 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. Fakturering skjer gjennom eget fakturaprogram.

Virksomheten benytter tre eksterne databehandlere, web-hotell hos WIX med domenenavn hos Domeneshop, journalsystem hos Microsoft OneNote, og regnskapssystem gjennom Conta Faktura. 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. Gunaketu Bjørn Kjønstad 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 for Pustepause.pdf» som vises til i klientavtalen og er tilgjengelig på virksomhetens web-sider.

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 i Pustepause.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 og kontaktopplysninger registreres i journalsystemet.

5.2.2 Journalføring

Det føres journal i journalsystemet etter hver konsultasjon.

5.2.3 Fakturering og oppfølging

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

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 eller brev.
3.	Terapeut	Hent personopplysninger fra OneNote.	Lagre som pdf
4.	Terapeut	Søk etter den registrerte i epostarkivet.	Skrive ut logg
5.	Terapeut	Søk etter den registrerte i filarkivet.	Hente registrerte skjema
6.	Terapeut	Legg alt, pluss dokumentet " Personvern - Oversikt over personopplysninger som behandles", i et ZIP-arkiv som passordbeskyttes. Alternativt skrive ut dokumentene.	Lage zip-arkiv
7.	Terapeut	Send ZIP-fil til den registrerte per epost eller sende i posten.	Per epost eller brev.
8.	Terapeut	Send passord til den registrerte per SMS.	Per SMS
9.	Terapeut	Slett ZIP-fil etter 14 dager.	Slette ZIP-fil

5.2.5 Korrigerings

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 korrigerings.	Per epost eller brev.
2.	Terapeut	Bekreft mottak og informer om tidsfrist (30 dager).	Per epost eller brev.
3.	Terapeut	Korriger personopplysninger i Klientopplysningsfilen og Fakturaprogrammet.	Korrigere
4.	Terapeut	Bekreft korrigerings.	Per epost eller brev.

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 eller brev.
3.	Terapeut	Slett personopplysninger i Klientopplysningssystemet ved å anonymisere eller pseudonymisere klientfilen.	Manuelt i Klientopplysningssystemet .
4.	Terapeut	Søk etter den registrerte i epostarkivet og slett all epost med unntak av 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 med unntak av epost som kan tenkes å være nødvendig for å håndtere en reklamasjon eller forsvare et rettskrav.	<fyll ut>
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 WIX

WIX behandler nettsiden til Pustepause. De videresender kontaktforespørsler. WIX har ingen separat databehandleravtale men har alle krav til dokumentasjon i henhold til GDPR i sin generelle avtale.

6.3 Conta Faktura og Microsoft Excel

Conta Faktura og Microsoft Excel leverer regnskapsprogram som Pustepause selv utfører regnskap med. Conta og Microsoft har ingen separat databehandleravtale men har alle krav til dokumentasjon i henhold til GDPS i sin generelle avtale.

6.4 Microsoft OneNote journalsystem>

Microsoft OneNote leverer journalsystem. Microsoft har ingen separat databehandleravtale men har alle krav til dokumentasjon i henhold til GDPS i sin generelle avtale.

7 Arkivering

Kontaktinformasjon og journalnotater arkiveres på PC med backup i OneDrive med passord og kryptert overføring. Epost arkiveres i Outlook. Brev og annen informasjon digitaliseres og arkiveres med kontaktinformasjon.

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 Gunaketu Bjørn Kjørstad som har tilgang til å registrere, endre og slette personopplysninger i egne systemer. Alle databehandlere oppdaterer personopplysninger kun etter instruks fra Gunaketu. Alle databehandlere har rutiner for sikkerhetskopiering og gjenoppretting av data.

8.3 Tilgjengelighet.

Det lagres personopplysninger lokalt på virksomhetens datautstyr som er passordbeskyttet. 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

10.1 Datatilsynet

Ved brudd på personvernet skal alltid Datatilsynet varsles. Varsling til Datatilsynet skal skje innen 72 timer etter at avviket ble oppdaget, via skjema i Altinn:

<https://www.altinn.no/skjemaoversikt/datatilsynet/melding-om-avvik-datatilsynet/>

10.2 De berørte

Varsling til de berørte skal skje når det er sannsynlig at avviket vil medføre en høy risiko for personvernet til de berørte. Det er virksomheten selv som gjør denne vurderingen. Varsling til de berørte skal skje så snart som mulig ved å bruke skjema i dokumentet "Personvern Varsling til de berørte ved avvik hos Pustepause.docx".

10.3 Rutine for avvikshåndtering

Følgende prosedyre skal følges:

Akt. Nr.	Hvem	Aktivitet	Hvordan
1.	Den som oppdager avviket.	Informere Terapeut.	
2.	Terapeut	Start avvikshåndtering.	Ser gjennom journal og fakturahåndtering.
3.	Terapeut	Lag en liste over hvem som er berørt.	Lage liste.
4.	Terapeut	Kartlegg mulige konsekvenser.	Vurdere tilgang til data
5.	Terapeut	Kartlegg mulige tiltak og iverksett umiddelbart om mulig.	Stoppe avvik og etablere nye sikre rutiner
6.	Terapeut	Fyll ut varslings skjema til Datatilsynet på Altinn .	Elektronisk skjema på Altinn.
7.	Terapeut	Vurder om det er sannsynlig at avviket vil medføre en høy risiko for personvernet til de berørte.	Ansvarlig vurderer ev. i dialog med Datatilsynet.
Hvis ja:			
8.	Terapeut	Fyll ut varslings skjema til de berørte.	Fyller ut

Pustepause

9.	Terapeut	Send skjemaet per epost til de berørte på listen.	Epost
10.	Terapeut	Iverksett eventuelle ytterligere tiltak.	Ved avdekkede behov
11.	Terapeut	Evaluer om iverksatte tiltak har lukket avviket.	Evaluer
Og uansett:			
12.	Terapeut	Dokumenter avviket, avviksbehandlingen og eventuelle tiltak for den årlige revisjonen.	Avviksskjema lagres i mappe: Pustepause/ administrasjon/ personvern

11 Internkontroll

Virksomheten har ikke behov for et omfattende internkontrollsystem. I tillegg til avviksprosedyren dokumentert over finnes det et egenkontrollskjema, dokumentet "Personvern Årlig egenkontroll xxxx Pustepause.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.