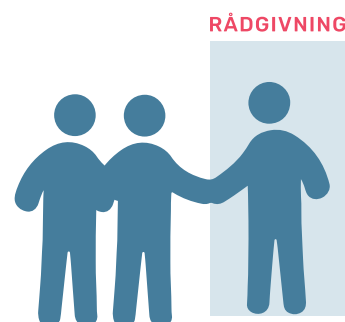


GUIDE TIL BEHANDLING AF PERSONOPLYSNINGER IFM. TELEFONISK OG DIGITAL RÅDGIVNING

Til sociale rådgivningstilbud der er
medlem af RådgivningsDanmark

GUIDE



INDHOLD

Introduktion / **3**

Anonymitet i rådgivnings- og dataretligt regi / **4**

Relevant behandlingsgrundlag / **5**

Sådan søges der tilladelse / **7**

Skabelon til ansøgning / **8**

INTRODUKTION

Denne guide er udarbejdet til sociale rådgivningstilbud, der er medlem af RådgivningsDanmark. Formålet med guiden er at understøtte medlemsorganisationerne i deres fortsatte rådgivningsarbejde samtidig med at sikre, at reglerne om behandling af personoplysninger overholdes.

Størstedelen af RådgivningsDanmarks medlemmer tilbyder telefon-, chat- eller brevkasse-rådgivning til rådsøgende. Der er typisk tale om anonym rådgivning, hvilket vil sige, at rådgivningstilbuddet ikke har adgang til brugernes personoplysninger – fx telefonnummer og IP-adresse – og således ikke kan identificere dem.

Den nye databeskyttelsesforordning og -lov trådte i kraft den 25. maj 2018 og er i vidt omfang en videreførelse af de gamle regler vedrørende behandling af personoplysninger. Det betyder blandt andet, at der også i dag i mange tilfælde skal søges om tilladelse hos Datatilsynet til behandling af følsomme personoplysninger i forbindelse med telefon- og chatrådgivning. Denne guide skitserer kort baggrunden for, hvorfor og hvornår der skal søges tilladelse til behandling samt indeholder en skabelon til, hvad ansøgningen skal indeholde.

ANONYMITET I RÅDGIVNINGS- OG DATARETLIGT REGI

Anonymitet har en ganske klar definition på rådgivningsfeltet. Det betegner den situation, hvor et rådgivningstilbud lover sine brugere, at rådgivningen og de enkelte rådgivere ikke har adgang til nogen personoplysninger om brugerne. Konkret betyder det fx, at rådgiveren ikke kan se brugerens telefonnummer, når telefonen ringer, ligesom rådgivningen heller ikke senere kan finde nummeret i de bagvedliggende tekniske systemer. Det vil til gengæld ofte være muligt for myndighederne, fx politiet, at finde frem til brugerens telefonnummer eller IP-adresse via tele- eller systemudbyderen. Men som sagt; da rådgivningen ikke kan se eller finde personoplysninger, er der altså tale om anonym rådgivning.

Anonymitet i dataretligt regi er imidlertid en anden størrelse. Anonymitet betegner her en fuldstændig anonymitet, der betyder, at ingen med nogen rimelige hjælpemidler kan få adgang til personoplysningerne. Ligesom det er en betingelse, at anonymiseringen er uigenkaldelig. Det vil sige, at man ikke kan af-anonymisere og finde tilbage til de oprindelige oplysninger. Er der tale om fuldstændig anonymitet, finder databeskyttelsesforordningen ikke anvendelse. Hvis fx politiet derimod kan finde frem til et telefonnummer eller en IP-adresse, er der ikke tale om anonymitet i dataretlig forstand. Der er derimod tale om, at rådgivningen pseudonymiserer brugernes personoplysninger, idet rådgivningen ikke selv kan se dem, men andre – potentielt – kan.

HVAD ER PSEUDONYMISERING?

Selv om oplysninger som et navn eller en adresse er erstattet af en kode, er det stadig en personoplysning, hvis det er muligt for nogen at føre koden tilbage til den oprindelige personoplysning. Pseudonymiserede oplysninger er omfattet af databeskyttelsesreglerne.

På samme måde betegnes flere enkeltstående oplysninger om en person, der i sig selv ikke er personhenførbare, men som tilsammen gør det muligt at identificere vedkommende, pseudonymiserede oplysninger.

KAN MAN UNDGÅ, AT TELE- OG SYSTEMUDBYDERE LIGGER INDE MED PERSONOPLYSNINGER?

Det vil ofte være teknisk muligt for udbydere af systemer til chatrådgivning at slette IP-adresser fuldstændigt. Det er imidlertid ikke nødvendigvis i samfundets – eller rådgivningens – interesse at frasige sig muligheden for at kontakte relevante myndigheder, fx i forbindelse med trusler om selvmord eller andre akutte situationer, med henblik på, at myndighederne kan tage affære.

Teleselskaber gemmer al kommunikation, det vil sige både telefonnumre og beskeder, således, at politiet – hvis nødvendigt – kan finde frem til det.

Derfor anbefaler RådgivningsDanmark, at rådgivninger identificerer et relevant behandlingsgrundlag for behandling af disse oplysninger, så det fortsat er muligt for rådgivningerne at leve op til underretnings- og afværgepligten på en meningsfuld måde.

RELEVANT BEHANDLINGSGRUNDLAG

Da brugernes personoplysninger ikke er anonyme i datarettlig forstand, er der tale om behandling af personoplysninger, hvilket betyder, at rådgivningen skal finde et behandlingsgrundlag for fortsat at kunne yde telefonisk og digital rådgivning.

Telefonnummer og IP-adresse betegnes som almindelige personoplysninger. Så er man i rådgivningen fuldstændig sikker på, at disse oplysninger ikke kan kobles med eventuelle følsomme personoplysninger, der måtte fremkomme under samtalen, skal man finde sit behandlingsgrundlag i databeskyttelsesforordningens kapitel 6.

Kan man derimod ikke forudse, hvorvidt telefonnummer og IP-adresse kan kobles med følsomme personoplysninger, der måtte komme frem under samtalen, fx oplysninger vedrørende psykisk eller somatisk sygdom eller seksualitet, skal rådgivningen finde et behandlingsgrundlag, der gælder for behandling af følsomme oplysninger.

HVAD ER FØLSOMME PERSONOPLYSNINGER?

Den juridiske betegnelse for de følsomme oplysninger er "særlige kategorier" af personoplysninger og er defineret i artikel 9 i databeskyttelsesforordningen. Følsomme oplysninger omfatter oplysninger om race, etnisk oprindelse, politisk, religiøs el. filosofisk overbevisning, fagforeningsmæssige tilhørsforhold, genetiske data, biometriske data mhp. entydig identifikation, helbredsoplysninger, seksuelle forhold eller orientering.

Artikel 9, stk. 2 i databeskyttelsesforordningen indeholder en række mulige behandlingsgrundlag, som man bør forholde sig til. I mange tilfælde vil det for rådgivningstilbud være særligt relevant at kigge på § 7, stk. 4 i databeskyttelsesloven:

Behandling af oplysninger omfattet af databeskyttelsesforordningens artikel 9, stk. 1, kan ske, hvis behandling af oplysninger er nødvendig af hensyn til væsentlige samfundsinteresser, jf. databeskyttelsesforordningens artikel 9, stk. 2, litra g. Tilsynsmyndigheden giver tilladelse hertil, hvis behandlingen efter 1. pkt. ikke foretages for en offentlig myndighed. Der kan i en tilladelse efter 2. pkt. fastsættes nærmere vilkår for behandlingen.

SÅDAN SØGES DER TILLADELSE

Der findes ikke en ansøgningsformular i forbindelse med ansøgning om tilladelse efter § 7, stk. 4. I stedet skal organisationen kontakte Datatilsynet per mail og heri beskrivelse en række forhold.

Mailen er første trin i ansøgningsprocessen og vil blive fulgt af en dialog med tilsynet, som typisk vil efterspørge yderligere oplysninger eller uddybning af det beskrevne. Jo flere oplysninger, der er med i første omgang, jo hurtigere og lettere er den videre dialog med og sagsbehandling hos tilsynet. Omvendt er der ikke tale om, at organisationen har én chance for at få tilladelse. Ansøgningen bliver altså ikke afvist, hvis der mangler informationer i første omgang.

Af mailen skal fremgå en relativ udførlig beskrivelse af:

- rådgivningstilbuddets målgruppe
- rådgivningstilbuddets tematik
- typer af behandlede personoplysninger
- kontaktoplysninger på kontaktperson i rådgivningen.

Derudover skal organisationen argumentere for

- nødvendigheden af behandlingen
- hvorfor det pågældende behandlingsgrundlag for behandlingen er det relevante.

Send ansøgningen til

Mailadresse: dt@datatilsynet.dk

Emnelinje: Ansøgning om tilladelse efter § 7, stk. 4

SKABELON TIL ANSØGNING

ANSØGNING OM TILLADELSE TIL BEHANDLING AF PERSONOPLYSNINGER IFM. [RÅDGIVNINGENS NAVN] RÅDGIVNING

Introduktion til organisationen og rådgivningstilbuddet

[Beskriv organisationen og det telefoniske eller digitale rådgivningstilbud, der søges tilladelse i forbindelse med.]

Rådgivningstilbuddets målgruppe

[Beskriv målgruppen for det telefoniske eller digitale rådgivningstilbud, der søges tilladelse i forbindelse med.]

Rådgivningstilbuddets tematik

[Beskriv det eller de temaer og problemstillinger, der rådgives om i det telefoniske eller digitale rådgivningstilbud, der søges tilladelse i forbindelse med.]

Typen af behandlede personoplysninger

[Beskriv hvilke typer personoplysninger, der behandles i det telefoniske eller digitale rådgivningstilbud, der søges tilladelse i forbindelse med. Dette vil være telefonnummer og/eller IP-adresse.

Beskriv desuden, hvilke følsomme personoplysninger rådgivningen, der typisk rådgives indenfor, fx somatisk eller psykisk sygdom eller seksuelle forhold.]

Hvilken behandling finder sted?

[Argumentér for, hvilken behandling, der er tale om, det vil sige alle de "håndteringer" af personoplysninger, der foretages.

Det vil her være relevant at skrive, at det drejer sig om behandling i form af dels *indsamling og opbevaring* af oplysningerne hos systemudbyder, dels potentiel *videregivelse* af oplysninger til myndighederne. Husk at have databehandleraftaler på plads med udbyderne af de tekniske systemer.]

Derfor er behandling, herunder videregivelse af oplysninger, nødvendig

[Argumentér for, hvorfor det er nødvendigt for rådgivningstilbuddet at kunne behandle – opbevare og videregive – de beskrevne personoplysninger.

Her vil det være relevant at skrive, at dét, at oplysningerne opbevares, er en forudsætning for at kunne videregive dem til myndighederne. Og videregivelsen er nødvendig ud fra væsentlige samfundsmæssige hensyn – at hjælpe sårbare borgere, der er i akut fare eller bringer andre

i fare. Uddyb fx med, at alle borgere – inklusiv ansatte og frivillige i rådgivningstilbud – har underretnings- og afværgepligt, og således er retligt forpligtet til at kontakte myndighederne i en række situationer. Dette er kun meningsfyldt, hvis myndighederne har en reel chance for at finde frem til de involverede personer – og hjælpe dem.

Beskriv desuden et par eksempler på typer af henvendelser og situationer fra egen rådgivning, hvor det er aktuelt, og beskriv hvad det kan betyde for brugeren, samfundet og rådgivningen, hvis rådgivningen *ikke* har mulighed for at behandle oplysningerne, og myndighederne dermed ikke har mulighed for at finde frem til dem.]

Derfor er § 7, stk. 4 det relevante behandlingsgrundlag

[Argumentér for, hvorfor § 7, stk. 4 er relevant som behandlingsgrundlag, herunder hvorfor andre behandlingsgrundlag ikke kan anvendes.

Det vil blandt andet være relevant at skrive, at rådgivningen sjældent kan forudse, hvilke typer personoplysninger, brugeren deler undervejs i samtalen, og derfor må rådgivningen – afhængigt af rådgivningens rådgivningstema – antage, at det kan være følsomme oplysninger, hvilket udelukker behandlingsgrundlag fra databeskyttelsesforordningens artikel 6.

Det vil ligeledes være relevant at beskrive, hvorfor det ikke er muligt at anvende samtykke som behandlingsgrundlag. Årsagen er, at det kræver, at brugeren identificerer sig selv – det vil sige underskriver samtykket – i forbindelse med afgivelse, hvilket vil sætte brugerens anonymitet over styr. Det vil oftest få den konsekvens, at brugeren trækker sig og ikke gennemfører rådgivningen.]

Guide til behandling af personoplysninger

ifm. telefonisk og digital rådgivning

© RådgivningsDanmark februar 2023

Læs mere

På www.raadgivningsdanmark.dk

Følg RådgivningsDanmark på [LinkedIn](#) og [Twitter](#)
eller tilmeld dig [nyhedsbrevet](#).



Email: info@raadgivningsdanmark.dk

Telefon: 61 31 70 28