Spør advokaten

GDPR – aldri for sent

Jeg har ikke kommet i gang med GDPR-arbeidet ennå. Er det for sent å gjøre noe nå, og hvor skal jeg eventuelt begynne?

Svar:

Det er aldri for sent. Virksomheter som ikke etterlever GDPR (General Data Protecion Regulation) kan bli bøtelagt av Datatilsynet, det har det vært flere eksempler på den siste tiden. Ved tilsyn vil det være av stor betydning om man har gjort sitt beste for å overholde regelverket. Det er av den grunn viktig å dokumentere det som er gjort.

Under følger en oversikt over det viktigste som må gjøres i den enkelte klinikk. Mer informasjon finnes tilgjengelig på www.tannlegeforeningen.no – jus og arbeidsliv – GDPR.

1. Lag en oversikt over hvilke personopplysninger som behandles i din virksomhet

Mal for protokoll finnes tilgjengelig for nedlasting på https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/protokoll-over-behandlingsaktiviteter/

Personopplysninger er enhver opplysning om en identifisert eller identifiserbar fysisk person. En person regnes som identifiserbar dersom det direkte eller indirekte er mulig å gjenkjenne ham eller henne basert på angitte opplysninger. Slike opplysninger kan for eksempel være navn og fødsels- og personnummer. Sensitive personopplysninger er typisk opplysninger vi anser som «private». Eksempler på sensitive personopplysninger er helseopplysninger, og også fagforeningsmedlemskap anses som en sensitiv personopplysning. I tannklinikker behandles det personopplysninger om pasienter og ansatte.

2. Sjekk at du har et lovlig grunnlag for behandling av personopplysningene

Regelverket skal sørge for at de som behandler personopplysninger gjør det på en måte som beskytter den enkeltes rett til privatliv. Derfor må man ha et behandlingsgrunnlag for å kunne behandle opplysningene.

Artikkel 9 nr. 2 bokstav h, jf. nr. 3, gir adgang til å behandle sensitive opplysninger i forbindelse med helsehjelp og forvaltning av slike tjenester. Opplysningene kan bare behandles under taushetsplikt. Tannlegers behandling av helseopplysninger om pasienter er underlagt omfattende regulering i særlovgivning, og vil falle inn under denne kategorien. Opplysninger om ansatte behandles oftest på grunnlag av avtale.

3. Sjekk at du følger regler og bransjenormer for behandling av personopplysninger i tannhelsetjenesten i dag

Gjeldende helselovgivning er i utgangspunktet i samsvar med GDPR. Bransjenormer, herunder «Norm for informasjonssikkerhet i helse- og omsorgssektoren», vil ha stor betydning også fremover, og det kommer en ny versjon i løpet av 2019.

4. Alle virksomheter må få på plass nye databehandleravtaler som er tilpasset GDPR

Der virksomheten beslutter å la andre behandle data på sine vegne, må det inngås databehandleravtale. Klinikkeiere må derfor sørge for at for eksempel leverandører av pasientjournalsystemer, lønnssystem o.l. har signert en godkjent databehandleravtale. Vi anbefaler NTFs avtalemal, men f.eks. Opus sin baserer seg på vår standard og kan inngå slik den foreligger. skal blant annet inneholde:
· hensikten med behandlingen · varigheten av behandlingen · behandlingens formål

5. Personvernerklæring
Alle virksomheter må ha en personvernerklæring, som f.eks. kan henges opp på venteværelset og legges ut på virksomhetens hjemmeside. Mal for personvernerklæring finnes tilgjengelig under GDPR-sidene på NTFs nettsted.

6. Implementer rutinene i virksomheten
Alle som jobber i lokalene/virksomheten må kjenne rutinene og følge dem. Se mer om dette i sikkerhetsinstruks for ansatte, i artikkelen «Introduksjon til personvern i arbeidsforhold» som ligger under GDPR-sidene på NTFs nettsted.

7. Sikre lovlig overføring av data
Norsk helsenett er den eneste godkjente måten for elektronisk overføring av helseopplysninger. Alternativet er ordinær postgang. Pasientjournaler kan sendes i vanlig post, men ikke på e-post uten å passordbeskytte vedlegget.

8. Vurdering av personvernombud
Alle virksomheter må vurdere om de må ha personvernombud. En «vanlig» tannlegevirksomhet trenger sannsynligvis ikke personvernombud, men bør dokumentere at det er vurdert. Se artikkelen «Trenger min virksomhet personvernombud» under GDPR-sidene på NTFs nettsted.

9. Sletting
Pasientjournaler skal oppbevares til det ikke lenger antas å være bruk for dem. Opplysninger om tidligere ansatte må slettes/makuleres, det som kan tas vare på er opplysninger om vedkommendes navn og ansettelsestid.

Silje Stokholm Nicolaysen
Juridisk rådgiver i NTF