NOF - GDPR
Retningslinjer for personvern og informasjonssikkerhet
For Osteopater MNOF

Versjon 001 – 30.06.2018

Utarbeidet av Einar C. Ellingsen fra Hammervoll Pind AS og Norges Landsforbund av Homøopraktikere (NLH).

Tilpasset med tillatelse- Norsk Osteopatforbund (NOF)

Innhold

1 Bakgrunn og formål

Hensikten med denne retningslinjen er å veilede og forenkle arbeidet til våre medlemmer med å overholde nye lovpålagte krav til personvern og informasjonssikkerhet. Bakgrunnen for retningslinjen er ny personvernlov basert på EU-direktiv, populært kalt GDPR (General Data Protection Regulation) som vil tre i kraft i Norge i 2018, og som stiller strengere krav til behandling av personopplysninger.
NOFs medlemmer forplikter seg til å følge de lover og regler som gjelder for autorisert helsepersonell, selv om mange osteopater pr. i dag står utenfor de regelverkene. GDPR vil, på samme måte som dagens personopplysningsregelverk, gjelde for alle som behandler personopplysninger, og dermed også for alle NOFs medlemmer. Dersom du allerede har på plass rutiner, systemer og sikkerhetstiltak som oppfyller de krav som ble stilt etter gammelt personvern-regelverk, er det ikke veldig store tilpasninger du har behov for å foreta deg.
Personopplysninger defineres som opplysninger om en identifiserbar fysisk person («den registrerte»). Det gjelder alle opplysninger og vurderinger som kan knyttes til en enkeltperson enten direkte eller indirekte. Med «behandling» menes enhver operasjon som utføres med personopplysninger, enten automatisert eller ikke, f.eks. innsamling, registrering, strukturering, lagring, tilpasning eller sammenstilling. Typisk for våre medlemmer vil være å registrere og lagre kundeinformasjon, samt notere og lagre helseinformasjon i forbindelse

med kundebehandlingen.
Våre medlemmer håndterer personopplysninger i forbindelse med sin virksomhet som behandler av pasienter. For vår standard virksomhet vil dette primært gjelde opplysninger som identifiserer kunden, samt kontaktinformasjon om kunden. Videre vil det gjelde ulike helseopplysninger og personlige opplysninger om kunden, som vil være nødvendig i behandlingen av kunden. Disse registreres og lagres i kundens e-journal i et for dette formål godkjent dataprogram hvor filer og informasjon ikke er tilgjengelig for uvedkommende. Det kan også tenkes at våre medlemmer har et register over tidligere, nåværende eller mulige pasienter. Det kan for eksempel være en e-post liste. Det er også noen som har registrert kontaktinformasjon om firma en samarbeider eller har avtaler med.
Loven krever at du som medlem har en rekke sikkerhetstiltak og overholder en hel del forpliktelser med tanke på hvordan du håndterer disse personopplysningene. De mest aktuelle kravene som du må oppfylle, både i ny og gammel lov, er beskrevet i denne retningslinjen. Det stilles blant annet krav til at du må ha egne skriftlige rutiner, ha et kontrollsystem og standardskjemaer. Dette for å dokumentere at du etterlever alle lovkrav. Vedlagt denne retningslinjen vil det ligge en standard rutine, som også har maler og standarder for de viktigste forhold som må dokumenteres.
Denne retningslinjen med vedlegg er tilpasset NOFs medlemmer som driver en «standard praksis», og herunder behandler personopplysninger slik beskrevet over. De standard dokumenter som er vedlagt er også tilpasset en slik standard virksomhet. Dette innebærer at våre medlemmer ikke vil få svar på alle spørsmål, men kun de viktigste og mest aktuelle krav. Dersom du behandler opplysninger på en særegen måte, må du kanskje iverksette ytterligere tiltak. Dette gjelder dersom du for eksempel har ansatte som du registrerer personopplysninger om, dersom du gir andre tilgang til de personopplysningene du har lagret, eller du har løsninger for registrering av personopplysninger fra kunden selv over nett. Dersom du har spørsmål eller behov for mindre tilpasninger kan du ta kontakt med NOF. For mer omfattende tilpasninger av dokumenter kan Einar C. Ellingsen hos advokatfirmaet Hammervoll Pind AS kontaktes. Vi gjør oppmerksom på at større tilpasninger utføres for medlemmets egen regning.
Du vil etter loven alltid selv være ansvarlig for behandlingen av de personopplysninger som du registrerer og lagrer (loven bruker begrepet: databehandlingsansvarlig). Dette vil gjelde selv om du engasjerer andre for å behandle dataene (typisk en IT-leverandør). Du er i tillegg ansvarlig for at de som behandler dataene på vegne av deg (loven bruker navnet: databehandler) overholder samme krav i loven som du må oppfylle. Det er derfor et krav i loven at du må inngå en avtale med slike databehandlere for å sikre at de også oppfyller krav og forpliktelser i loven.
Etter ny lov er det ikke lengre krav til konsesjon eller meldeplikt til Datatilsynet. Det nye regelverket forutsetter at alle som behandler personopplysninger selv sørger for at de oppfyller lovkravene for slik behandling. Datatilsynet vil foreta kontroller av etterlevelsen, herunder vil de kunne komme på uanmeldte tilsyn hos deg. Etter nytt regelverket vil brudd på loven kunne få store konsekvenser i form av økt bøtenivå (kan bli hele 4 prosent av omsetning).
Som vedlegg 1 til denne retningslinjen følger et standard dokument for en skriftlig rutine som våre medlemmer må ha på plass for å etterleve lovens krav til dokumentasjon. Hvert medlem må se igjennom dette dokumentet, og eventuelt foreta de tilpasninger som er nødvendig for dem. Deretter skriver medlemmet inn navn på virksomheten og dokumentet dateres som virksomhetens egen policy og rutine.
Som vedlegg til dette dokumentet (vedlegg 1) følger også de mest sentrale dokumenter og skjemaer som hvert medlem må ha for å oppfylle lovens krav. Når og hvordan disse skjemaene skal benyttes vil bli forklart i denne retningslinjen. Det er det enkeltes medlems ansvar å, ved behov, å fylle ut og tilpasse disse standardene og malene til den virksomhet og

aktivitet som den enkelte driver med.
I det følgende vil vi gå igjennom de mest sentrale krav i ny lovgivning og forklare hva våre medlemmer må gjøre for å oppfylle disse kravene.

2. Krav om skriftlig oversikt over behandlingen av personopplysninger

Det første, og mer overordnede kravet, innebærer at alle som behandler personopplysninger må foreta en skriftlig kartlegging av hvordan de bruker personopplysninger. I praksis medfører dette at alle medlemmer må utarbeide en oversikt over hvilke personopplysninger en behandler, hvorfor en behandler disse opplysningene, hvordan en behandler disse og hvem som har tilgang.
Typisk vil personopplysningene som medlemmene lagrer være kontaktinformasjon til pasienter, samt visse opplysninger knyttet til kundens helse, personlige forhold og behandlingsopplegg. Det er viktig under dette kravet å få oversikt over de sensitive opplysninger som en lagrer og hvordan de er lagret. Sensitive personopplysninger ansees å være blant annet opplysninger om rasemessig eller etnisk bakgrunn, eller politisk, filosofisk eller religiøs oppfatning, at en person har vært mistenkt, siktet, tiltalt eller dømt for en straffbar handling, helseforhold, seksuelle forhold eller medlemskap i fagforeninger.
For våre medlemmers virksomhet vil sensitive personopplysninger som behandles først og fremst være innenfor kategorien «helseforhold». Alle typer opplysninger som omhandler eller kan relateres til en pasients helseforhold vil måtte kategoriseres som sensitive personopplysninger, for eksempel opplysninger om hvor vedkommende har vondt/har plager fysisk eller psykisk, hvilke medisiner, diagnoser og behandling vedkommende har fått/får, personlige og andre forhold som kan ha betydning for helsen, mv.
En kartlegging som her kreves trenger ikke å være omfattende eller komplisert. Det sentrale i kravet er at du tenker igjennom alle personopplysninger du har registrert og lagret, for å kartlegge ovennevnte forhold. For våre medlemmer, hvor type opplysninger som behandles og måten de behandles på er begrenset, vil en slik oversikt kunne gjøres kort og skjematisk. Vedlagt standard rutinen følger det et standard skjema for utfylling med eksempler på hvordan du kan beskrive aktuell bruk.
Kartleggingen bør minimum omfatte:

- Hvilke aktiviteter som innebærer behandling av personopplysninger
- Hvilke typer personopplysninger som samles inn
- Formålet med behandlingen og behandlingsgrunnlaget (rettslig grunnlag)
- Hvor behandlingen/lagringen finner sted (typisk IT-system eller fysisk arkiv (ikke anbefalt))
- Hvor personopplysningene oppbevares (fysisk og lokasjon eller nett)
- Eventuell bruk av databehandler (som for eksempel er en IT-leverandør)

Når du har fått oversikt over hvilke behandlinger av personopplysninger som skjer i virksomheten, vil du lettere kunne vurdere om det er nødvendig å lagre disse opplysningene i fremtiden, og i så fall hva som er ditt rettslige grunnlag for dette i dag, eventuelt om du må innhente et samtykke fra kunden.

3. Krav om at personopplysningene håndteres på en sikker måte

Ny lov krever at alle som behandler personopplysninger må ha en rutine for hvordan personopplysninger innhentes, registreres, informeres, oppbevares og slettes, som vil sikre at opplysningene ikke kommer på avveier, blir misbrukt eller ødelagt. Du må kunne dokumentere tilstrekkelige informasjonssikkerhetstiltak for alle de personopplysninger du har lagret.
Tiltakene som kreves skal ivareta prinsippene i loven om forholdsmessig sikring av konfidensialitet, integritet, tilgjengelighet og kvalitet på de opplysningene. Krav om konfidensialitet innebærer blant annet at alle personopplysninger skal være sikret mot

uautorisert innsyn og tilgang fra andre. Det er strengere krav for sikring av sensitive personopplysninger, som for eksempel helseopplysninger, enn andre type personopplysninger. Krav om integritet og kvalitet innebærer at opplysningene skal være sikret mot uautorisert og uønsket endring eller sletting, samt at opplysningene skal være korrekte og oppdaterte. Herunder ligger et krav om at det tas sikkerhetskopier som oppbevares trygt. Krav om tilgjengelighet innebærer at en må sikre at opplysningene er tilgjengelig for de som skal ha tilgang når de trenger dem. Opplysningene skal også være mulig å utlevere innen kort tid til den registrerte.
Loven krever at det utarbeides sikkerhetsmål for behandlingen av personopplysninger i virksomheten, og en strategi (tiltak) for å nå disse målene. Medlemmene må videre ha konkrete krav til IT-sikkerheten som må beskrives i en rutine. Medlemmets sikkerhetsmål og –strategi, samt detaljerte krav til IT-sikkerhet følger av standard rutinen (vedlegg 1).
Følger medlemmet de krav som er beskrevet, og personopplysningene lagres lokalt på pc/ server/mobilt utstyr som ikke har tilgang til nettverk/internett, vil det være begrenset med ytterligere sikkerhetstiltak som må vurderes og etableres for våre medlemmer.
Kravene til IT-sikkerhet er mer utfordrende å etterleve dersom personopplysninger lagres på en datamaskin/server/mobilt utstyr med tilgang til nettverk/internett eller til eksterne lagringsmedium. Har medlemmet en slik løsning og du er usikker på om IT-sikkerheten er ivaretatt anbefales det å innhente profesjonell IT-bistand. Benyttes trådløse nettverk vil dette være sårbart i forhold til påkobling fra uvedkommende, dersom IT-sikkerheten ikke blir godt ivaretatt. Medlemmet må derfor påse at trådløst nettverk er sikret mot påkobling fra andre.
4. Krav om risikovurdering, kontroller og konsekvensvurdering

Risikovurdering
Når en har fått kartlagt hvilke personopplysninger en har lagret (se første krav i punkt 2 over), er det også krav til at en vurderer om måten å lagre opplysninger i dag er sikker nok. Altså om sikkerheten er tilstrekkelig sett i forhold til den type personopplysninger en behandler.
Risikoen som skal kartlegges er sannsynlighet for og eventuelt konsekvenser av uønskede hendelser, typisk dersom uvedkommende for tilgang til opplysningene eller at de slettes eller kommer på avveier.
Hensikten med en risikovurdering er å finne ut om det er områder hvor det er behov for å iverksette flere eller andre sikkerhetstiltak for å etterleve personvernreglene. Er kartlagt risiko høyere enn det som er ansett som en akseptabel risiko må det gjennomføres nye tiltak.
Som vedlegg til standard rutinen følger et skjema for en enkel risikovurdering, med de mest aktuelle eksempler for beskrivelsen av risikoen basert på den behandlingen som er standard og anbefalt for våre medlemmer. Skjemaet må fylles ut av ut av alle databehandlingsansvarlige og oppdateres årlig.
Vurdering av personvernkonsekvenser
Dersom du foretar endringer i hvordan du behandler personopplysninger, for eksempel dersom du går fra fysisk arkiv til lagring på datamaskin eller installerer nytt IT-system, stiller loven krav til at en vurderer hvilke konsekvenser dette vil kunne ha for de personopplysningene du behandler. En slik vurdering må du i så fall gjøre skriftlig slik at dette kan dokumenteres i etterkant.
Krav til egenkontroll med IT-sikkerheten
Du skal hvert år foreta en kontroll av at IT-sikkerheten ivaretas og er tilstrekkelig. Du må ha en kort skriftlig plan som sier når og hvordan en slik kontroll skal utføres.
Kontrollen skal i henhold til loven minimum omfatte en vurdering av virksomhetens lagring av personopplysninger, dagens sikkerhetstiltak og eventuell bruk av leverandører. Inkludert i en slik kontroll må du vurdere om de sikkerhetsmål og -strategier, samt om ditt IT-systemet er godt nok. Rutine for håndtering av personopplysninger og for informasjonssikkerhet bør gjennomgås jevnlig.

5. Krav om rettslig grunnlag og et formål med behandlingen

For all behandling du gjør av andres personopplysninger må du først ha fått lov til å gjøre den. Dette kalles å ha et rettslig grunnlag for behandlingen. Dersom du ikke har et slikt rettslig grunnlag vil din registrering og lagring av slike opplysninger være ulovlig.
Et rettslig grunnlag kan blant annet være en lovbestemmelse som gir deg tillatelse til å innhente og behandle opplysninger om andre. Det kan også være en avtale du har med det individ personopplysningene gjelder for («den registrerte»), som innebærer at du må behandle opplysninger om denne personen for å oppfylle avtalen. Typisk dersom du har avtalt at du skal behandle en kunde og sende regning, må du ha lov til å registrere navn og kontonummer. I visse tilfeller kan det rettslige grunnlaget for å lagre opplysningen basere seg på en samfunnsinteresse mv. Et annet rettslig grunnlag er samtykke fra den registrerte om å kunne behandle personopplysninger om denne.

NOF krever at alle medlemmer følger samme regler som for autorisert helsepersonell, men behandling av personopplysninger for osteopater har ikke grunnlag i egne lovbestemmelser eller spesielle samfunnsinteresser. Vi må da enten basere oss på en avtale med våre pasienter eller innhente et samtykke. For kontakt- og identifikasjonsinformasjon vil den avtalen som er inngått med kunden, om å behandle vedkommende, være godt nok rettslig grunnlag. Behandling av slike opplysninger vil være nødvendig for å oppfylle den avtalen en har med kunden. For sensitive personopplysninger, som vi har behov for i behandlingen (for eksempel helseopplysninger, informasjon om medisinering og personlige forhold), er det delte meninger om hva som må gjøres. I dokumentene vi har fått fra advokaten og NLH mener de at medlemmet må innhente skriftlig samtykke fra kunden for å lagre sensitive personopplysninger. De mener videre at en generell avtale med kunden ikke gir rettslig grunnlag for å behandle sensitive personopplysninger og løser dette ved å ha skriftlig avtale på å lagre slike opplysninger. Siden NOFs medlemmer er pålagt å bla. følge lov for helsepersonell og forskrift om journalføring, mener vi at det er nok rettslig grunnlag med muntlig informert samtykke for osteopater å registrere sensitive personopplysninger i pasientens journal.
At samtykket er "informert" betyr at det må være avgitt frivillig, men en uttrykkelig erklæring fra kunden om at han eller hun godtar behandling av opplysninger om seg selv. Det stilles krav til at du må informere om hvorfor du trenger å lagre opplysningen, hvordan du lagrer de, samt om kundens rettigheter til opplysningene og innsyn i disse mv. Kravet til informert samtykke skal dokumenteres. Mangler kunden samtykkekompetanse (typisk er mindreårig) gjelder spesielle regler for samtykke.
Det er et krav at det er et klart formål med den registreringen og lagringen av personopplysninger du gjør. For våre medlemmer vil dette enten være begrunnet i behov for å administrere kundeforholdet (altså at det trengs blant annet informasjon om navn og kontaktinformasjon til kundene) eller det vil være nødvendig for å kunne foreta en forsvarlig behandling og oppfølging av kunden (at det er nødvendig å ha informasjon om helseforhold, medisinering og en del personlige forhold).
Det er i loven også et krav om at personopplysningene som er innhentet/registrert til et formål ikke kan benyttes til andre formål senere, uten at du har skaffet et nytt rettslig grunnlag for dette. Medlemmer av NOF er pålagt å følge de samme kravene som autorisert helsepersonell, og skal oppbevare journalen i henhold til dette (minst 10 år).
Ved markedsføring og salg av varer og tjenester via mail, sms, nyhetsbrev etc. er det egne regler som gjelder. Dersom dataansvarlig ønsker å sende kunden/pasienten tilbud på varer eller tjenester krever loven at må du innhente skriftlig samtykke til dette! (Elektronisk personlig bekreftelse kan også fungere i noen systemer). En standard samtykkeerklæring som du må tilpasse din virksomhet kan ettersendes ved henvendelse til NOF.

6. Krav om hendelses- og avvikslogg og varslingsplikt

GDPR stiller, som gjeldende lov, et krav om at avvik fra lovlig måte å behandle personopplysninger fanges opp og registreres. Det vil si at det enkelte medlem må sørge for å ha en rutine som sikrer registrering dersom personopplysninger kommer på avveier, blir slettet uten grunn, ikke er korrekte eller blir brukt til annet formål enn de var innhentet for. I tillegg bør hendelser som kan ha betydning for sikkerhet o.l. loggføres. Dette kan være endringer i hvem som er brukere og/eller har tilgang til systemet mv. og endringer i tilgang til nettverk mv. En slik rutine må også si noe om hvordan alvorlige hendelser skal håndteres dersom de oppstår.
Ny lov stiller også et klart krav om at myndighetene må varsles dersom personopplysninger kommer på avveier eller det ellers skjer ulovlig behandling. Et slikt varsel skal gis uten ugrunnet opphold. Det er også et krav at de registrerte varsles i slike tilfeller.
Vedlagt standard rutinen følger et eget skjema for registrering og eventuelt rapportering av avvik og hendelser, som også sier noe om hvordan en skal håndtere alvorlige hendelser.
Formålet med avviksbehandling er å sikre at:

- sikkerhetsbrudd håndteres på en systematisk måte
- normaltilstanden gjenopprettes etter et sikkerhetsbrudd
- endringer i sikkerhetsarbeidet vurderes for å hindre framtidige sikkerhetsbrudd
- Datatilsynet varsles ved uautorisert utlevering av helse- og personopplysninger

7. Styrkede rettigheter for den registrerte

I den nye personvernforordningen er det en rekke styrkede rettigheter for den registrerte med tanke på krav på informasjon om behandlingen av opplysningene som gjøres, og krav om selv å ha kontroll over disse opplysningene. Dette betyr at våre medlemmer må vite hva som det skal informeres om og hvordan en skal håndtere anmodninger om innsyn fra pasienter. Dette følger informasjon om i standard rutinene.

<u>Innsyn</u>

Det er først og fremst økte forpliktelser til å gi informasjon om hva en registrerer og til innsyn i det som er registrert. De registrerte skal også informeres når det samles inn personopplysninger om vedkommende fra andre.
Det legges til grunn at våre medlemmer kun innhenter personopplysninger fra medlemmet selv, og at det i den anledning gis informasjon om at personopplysninger registreres og lagres ved start av kundeforholdet (ved informert og muntlig samtykkeerklæring). Det er derfor ikke behov for å ha en egen rutine eller skjema for hvordan de registrerte skal informeres om innhenting av personopplysninger. I det tilfelle at et medlem innhenter personopplysninger fra andre enn kunden, og kunden ikke er informert om dette, må kunden informeres om dette.
Det er også et krav i loven om «dataportabilitet», som innebærer at den registrerte skal kunne be om å få sine data utlevert, slik at en kan ta det med seg disse til en annen tilbyder.
Før personopplysninger gis innsyn i, bør medlemmet kreve at anmodningen om innsyn er skriftlig og undertegnet. Personen som spør må videre klart kunne identifisere seg selv, slik at en er sikker på at en ikke utleverer informasjon til uvedkommende og dermed bryter taushetsplikten. Skal informasjonen sendes til vedkommende så bør det sendes til den adressen som er registrert i registeret, alternativt til folkeregistret adresse.
Det legges til grunn at våre medlemmer ikke utleverer personopplysninger til andre enn den registrerte selv. I den grad noen medlemmer gjør dette, må dette utføres under strenge krav til vurdering og orientering til den registrerte. Det bør etableres egen rutine for dette og innhentes juridisk råd før taushetsbelagte personopplysninger utleveres til andre enn den registrerte selv.

<u>Korrekte og oppdaterte</u>

Det er også et krav om at de opplysningene som registreres og lagres er korrekte og holdes

oppdaterte. Medlemmet har plikt til uoppfordret å sørge for at opplysninger som behandles er riktige, herunder at det foretas nødvendig oppdatering og retting.
Kundens adresse og kontaktopplysninger bør derfor jevnlig oppdateres. Det viktigste er imidlertid at registrerte opplysninger om kunden som er nødvendig for behandlingen holdes oppdaterte i løpende kundeforhold. Riktigheten av informasjonen som føres i journalen bør sjekkes jevnlig under et behandlingsforløp og før hver ny behandling starter. For eksempel kan dette være opplysninger om ny medisinering eller nye diagnoser på kunden.
De nye reglene gir også økte rettigheter til de som er registrert til å kreve retting av opplysninger som er feil.
Det er medlemmet selv som må vurdere om det er adgang til å rette eller slette opplysninger i journalen og som må utføre korrigeringen/suppleringen som er krevd. Kommer en anmodning om retting av uriktige opplysninger fra kunden, skal retting skje straks, med mindre det er grunn til å betvile at henvendelsen kommer fra den registrerte eller at det som opplyses er korrekt.
Kravet til oppdatering og retting innebærer at opplysninger som benyttes i vår behandling av pasienter må være oppdaterte og gi i et riktig bilde at dagens helsesituasjon mv. Kravet til oppdatering og retting innebærer at opplysninger som er benyttet tidligere ikke kan slettes, men nye opplysninger skal legges inn med ny datering og beskrivelse av hva som faktisk er riktig. (" Viser til journalnotat fra "dato" – denne føringen var feil og den riktige er som følger: ..."

Sletting når grunnlaget og/eller formålet bortfaller
NOFs medlemmer forplikter seg til å følge de lover og regler som gjelder for autorisert helsepersonell når det gjelder oppbevaring og sletting av pasientopplysninger. Sletting av sensitive helseopplysninger kan gjøres etter 10 år dersom de ikke antas å ha nytte for pasienten.
For mer info se Lov om helsepersonell m.v. (helsepersonelloven), Lov om behandling av personopplysninger (personopplysningsloven) og forskrift for journalføring
8. Krav når en benytter leverandør eller samarbeidspartnere

Dersom andre skal ha tilgang til eller behandle personopplysninger medlemmet selv har lagret, må en forsikre seg om at disse også oppfyller lovens krav til behandling av personopplysninger. Dette vil typisk kunne være en IT-leverandør som lagrer dine kundedata på sin server eller har tilgang til din datamaskin/server, eventuelt en samarbeidspartner som har tilgang til ditt arkiv om dine pasienter.
I slike tilfeller stiller loven krav om at en må inngå en såkalt databehandleravtale. I en slik avtale skal det stilles krav til leverandøren/samarbeidspartneren når det gjelder behandlingen av personopplysninger og sikkerheten rundt dette. Det sentrale med dette kravet er at medlemmet fortsatt står ansvarlig for at loven etterleves selv om andre behandler personopplysningene. Du har trolig fått en kopi av slik databehandleravtale og signert på den fra din IT-leverandør. Ta vare på den som dokumentasjon.
En del IT-leverandører som tilbyr eksterne serverløsninger for lagring av medlemmets data, kan ha såkalte «skytjenester»/servere lokalisert i annet land enn Norge. Det er viktig å være klar over at det er egne krav i loven til overføring av personopplysninger til utlandet. Ved overføring av personopplysninger til utlandet må medlemmet selv påse at krav i loven følges av IT-leverandør.
9. Etterlevelse og kontroll

Den enkelte dataansvarlige plikter til enhver tid å følge de gjeldende lover og regler, samt retningslinjer og standard rutine for kontroll, samt å jevnlig oppdatere skjemaer og rutiner slik at de gjenspeiler praksisen som utføres.