Veiledning for NTFs medlemmer om GDPR, personvern og nye krav til behandling av personopplysninger. Ofte stilte spørsmål og svar.

Innhold

1. Innledning

Denne veiledningen er ment å gi en oversikt over mange av de problemstillingene som er aktuelle i forbindelse med GDPR («General Data Protection Regulation») og innføring av strengere krav til behandling av personopplysninger fra 25. mai 2018. Veiledningen er generell og kan ikke anses som uttømmende. Den er kun ment å gi en generell innføring og grunnleggende kjennskap til hva GDPR innebærer, og hva den enkelte eventuelt må foreta seg, fordi dette må tilpasses den enkelte virksomhet. Se også NTFs sjekkliste for personvern for å sikre at din virksomhet er godt nok forberedt.

Alle som har spørsmål eller har behov for ytterligere veiledning, anbefales å ta kontakt med Datatilsynet, se også informasjon på www.datatilsynet.no.

2. Hva er personvern?

Personvern handler om retten til et privatliv og retten til å bestemme over egne personopplysninger. Grunnpilaren er at alle mennesker har en ukrenkelig egenverdi. Som enkeltmenneske har du derfor rett på en privat sfære som du selv kontrollerer, hvor du kan handle fritt uten tvang eller innblanding fra staten eller andre mennesker.

Prinsippet er blant annet forankret i Den europeiske menneskerettighetskonvensjonen, EMK, art 8, hvor det heter: *«Enhver har rett til respekt for sitt privatliv og familieliv, sitt hjem og sin korrespondanse.»* Bestemmelse om personvern er også tatt inn i Grunnloven § 102 som sier at *«Enhver har rett til respekt for sitt privatliv og familieliv, sitt hjem og sin kommunikasjon. Husransakelse må ikke finne sted, unntatt i kriminelle tilfeller. Statens myndigheter skal sikre et vern om den personlige integritet.»*

Personvernbegrepet innebærer ikke bare rett til vern av privatlivets fred og den enkeltes personlige integritet, men også i stor grad vern av individers rett til å ha innflytelse på bruk og spredning av personopplysninger om seg selv. Den enkelte skal i størst mulig grad kunne bestemme over sine egne personopplysninger.

3. Hvorfor er det mye snakk om personvern og GDPR?

Samfunnet har i de senere år vært i en radikal digital endring. Den digitale utviklingen har gått fort, og det eksisterende lovverket har ikke vært tilpasset dagens utfordringer. EU har derfor gått inn for å styrke privatpersoners rettigheter og skjerpe bedriftenes forpliktelser.

Personvernforordningen GDPR er et regelsett som ble vedtatt av EU i april 2016. Regelsettet bestemmer hvordan det offentlige og bedrifter kan og skal behandle personopplysninger. Videre gir det rettigheter for enkeltpersoner direkte overfor det offentlige og bedrifter når det gjelder personopplysninger som har blitt samlet inn om dem.

Reglene skal gjelde i hele EU og EØS-området fra og med den 25. mai 2018. Forordningen innebærer en full harmonisering av personvernregelverket i EU/EØS. Norske myndigheter har foreslått å innføre GDPR ved inkorporasjon. Forordningen vil dermed gjelde som norsk rett slik som den er. Departementet har foreslått en videreføring av gjeldende regler på områder hvor det er anledning til nasjonale tilpasninger.

4. Gjelder reglene for min bedrift, og hva må vi gjøre nå?

Ja, alle virksomheter og privatpersoner får nye regler å forholde seg til fra og med 25. mai 2018. Reglene gjelder for alle som behandler personopplysninger. Det er ikke mulig å drive tannlegevirksomhet uten å behandle personopplysninger.

Det første som må gjøres er at bedriften skaffer seg en oversikt over hvilke personopplysninger som behandles. Det bør lages en oversikt over hvilke personopplysninger det er snakk om, hvor opplysningene kommer fra samt hva som er det rettslige grunnlaget for behandlingen av de aktuelle personopplysningene. Den enkelte bedrift ligger godt an til å tilpasse seg de nye reglene dersom en følger de reglene som gjelder for tannlegevirksomheter i dag. Det er derfor viktig å kontrollere at de reglene som allerede gjelder overholdes.

GDPR omfatter imidlertid all behandling av personopplysninger i virksomheten, ikke bare i forhold til pasienter. Se mer om dette under punkt 7 «Hva gjør jeg med de andre personopplysningene i virksomheten?»

5. Regler og bransjenormer for behandling av personopplysninger i tannhelsesektoren i dag

Personopplysningsloven gjelder generelt. Behandling av helseopplysninger har imidlertid behov for et særskilt vern, og reguleres også i dag i stor grad av særlovgivning, bl.a. helseregisterloven, helsepersonelloven og pasientjournalloven.

Det er i tillegg egne normer som gjelder for tannhelsetjenesten i dag, som det forutsettes at alle tannlegevirksomheter følger.

Bransjenorm for informasjonssikkerhet og personvern i helse- og omsorgstjenesten v5.3 som også omfatter tannklinikker.

Personvern og informasjonssikkerhet for virksomheter i tannhelsetjenesten v2, og en mal for internkontroll v1.3.

Det er også en veileder med avtaleeksempel om samarbeid mellom virksomheter om felles journal –, som vil gjelde i de fleste samarbeidsforhold mellom praksiseier og assistenttannleger, se mer om dette under punkt 16 «Har dette betydning for forholdet mellom praksiseiere og assistenttannleger?».

6. Vil reglene og bransjenormene for tannhelsetjenesten bli endret på grunn av GDPR?

GDPR åpner i stor grad for særregler når det gjelder behandling av helseopplysninger i helsesektoren. Helse- og omsorgsdepartementet legger til grunn at gjeldende lover og forskrifter om behandling av helseopplysninger i utgangspunktet er i samsvar med GDPR. Det vil imidlertid bl.a. bli foreslått lovtekniske endringer.

GDPR åpner for bransjenormer som skal bidra til etterlevelse av forordningen. En bransjenorm er retningslinjer for hvordan en sektor/bransje skal sikre at den behandler personopplysninger på en riktig og god måte. *Norm for informasjonssikkerhet i helse og omsorgstjenesten (Normen)* er et slik omforent sett av krav til informasjonssikkerhet. Bransjenormene skal godkjennes av Datatilsynet. Normen vil med andre ord også fremover kunne være en måte å etterleve kravene til sikkerhet ved behandlingen.

Normen revideres av Styringsgruppen for Normen, hvor NTF deltar, og vil komme i en versjon som er tilpasset GDPR. Normen v5.3, en foreløpig versjon med enkelte GDPR-krav, ventes ferdig 31. mai 2018. Normen v6.0, med nye og endrede krav fra GDPR, ventes ferdig i første kvartal 2019. Vi vil komme med oppdatert informasjon når nye versjoner blir tilgjengelig

GDPR artikkel 32 og 40

7. Hva gjør jeg med de andre personopplysningene i virksomheten? Risikovurdering og rutiner for informasjonssikkerhet og internkontroll

GDPR omfatter all behandling av personopplysninger i virksomheten, ikke bare i forhold til pasienter, men også leverandører, ansatte mv. Dere må derfor sette dere inn i det nye regelverket og lage rutiner for å følge de nye reglene.

Den enkelte virksomhet har ansvar for å gå gjennom, oppdatere og samle de rutiner man har for informasjonssikkerhet og internkontroll.

Opplysningene i virksomheten skal sikres med hensyn til:
- Konfidensialitet - uvedkommende får ikke tilgang på opplysningene,
- Integritet - opplysningene endres ikke uautorisert eller utilsiktet,
- Tilgjengelighet - opplysningene er tilgjengelige når det er behov for dem.

Regelmessige gjennomganger skal sikre:
- At mål for behandling av personopplysninger oppnås
- At korrigerende tiltak gjennomføres for å sikre at behandlingen av personopplysninger skjer innenfor lov- og regelverk, herunder virksomhetens rutiner. Resultatene fra egenkontroll og avviksbehandling gjennomgås og sammenlignes med de korrigerende tiltakene.
- At internkontroll og styringssystem for informasjonssikkerhet er hensiktsmessige og tilstrekkelige, og tilfredsstiller lovbestemte krav

Sikkerhetsmål for den enkelte virksomhet kan ta utgangspunkt i følgende:
1) Informasjon skal kun behandles i henhold til gjeldende lovgivning, adferdsnormer og sertifiseringer som gjelder for virksomheten.
2) Sikkerheten skal ivaretas som en integrert del av virksomheten.
3) Fysiske tiltak skal hindre at uautoriserte får adgang til lokaler der personopplysninger og andre opplysninger kan være lagret og behandles.
4) Tilgang til systemer og informasjon gis kun til medarbeidere ved behov («need to know»). Det forhindres at uvedkommende får tilgang til systemer og informasjon.
5) Informasjonsbehandling skal være korrekt. Informasjon skal ikke forandres uten lovlig tilgang
6) Systemer, tjenester og informasjon skal være tilgjengelig til rett tid for autoriserte personer
7) Rutiner for å håndtere uønskede/virksomhetskritiske hendelser tas i bruk. Uønskede hendelser skal kunne spores.
8) Medarbeidere som bruker virksomhetens informasjonssystemer og behandler personopplysninger, skal ha tilstrekkelig kompetanse for å ivareta sikkerhetsbehov og -krav.

Se for øvrig punkt 15 «Har dette betydning for mine ansatte?»

8. Hvor finner jeg reglene om personopplysninger, og hva gjelder reglene for?

Det vil komme en ny personopplysningslov som følge av GDPR. Se regjeringens forslag til ny personopplysningslov på www.regjeringen.no.

Reglene gjelder for «behandling av personopplysninger». Kort sagt regnes nesten enhver befatning med personopplysninger som en «behandling». Se mer under punkt 11 «Hva er behandling av personopplysninger?».

Gjeldende regler er personopplysningsloven med tilhørende forskrift. Regler om personopplysninger i særlovgivning for helsetjenesten går foran personopplysningsloven, se over.

EUs forordning, GDPR, finnes i en foreløpig norsk oversettelse i en nedlastbar pdf på Datatilsynets nettsider.

9. Hva er en personopplysning?

Personopplysninger er **enhver** opplysning om en identifisert eller identifiserbar fysisk person («den registrerte»). Dette innebærer at personopplysningene må relatere seg til en bestemt person, og ikke grupper. Dette kan eksempelvis både være opplysninger om ansatte og pasienter.

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, fødsels- og personnummer (ID-nummer), fingeravtrykk, lokasjon eller online kjennetegn som IP-adresser. Det kan også dreie seg om en eller flere faktorer som personens fysiske, genetiske, mentale, økonomiske, kulturelle eller sosiale identitet.

Andre eksempler på personopplysninger er kallenavn, alder, kjønn, høyde, vekt, øyefarge, foto, familiære forhold, sivil status etc. Videre regnes utdanning, seksuelle forhold, domfellelse for straffbare forhold, medlemskap i fagforening, nåværende og tidligere arbeidssted, formue, gjeld, inntekt, bilnummer, kjøps- og betalingshistorikk, adresse, passnummer, og e-postadresse som personopplysninger.

Det er viktig å være klar over at det ikke kun er faktaopplysninger som er personopplysninger. Vurderinger som er gjort om en person anses også som personopplysning. Videre er opplysninger å anse som personopplysning selv om de hverken er hemmelige eller kan være å anse som personlige slik som for eksempel telefonnummer. Også opplysninger om adferdsmønstre er å anse som personopplysning. Opplysninger om hva du handler, hvilke butikker du går i, hvilke tv-serier du ser på, hvor du beveger deg i løpet av en dag og hva du søker etter på nettet er alt sammen å anse som personopplysninger.

Opplysninger om bedrifter slik som for eksempel årsregnskap og kontaktopplysninger er ikke personopplysninger. Opplysninger om ansatte er derimot personopplysninger. Se mer om dette under punkt 15 «Har dette betydning for mine ansatte?»

GDPR artikkel 4 nr. 1, ft. 27, 158 og 160

10. Hva er «særlige kategorier» /sensitive personopplysninger?

Sensitive personopplysninger er typisk opplysninger vi anser som «private». Eksempler på sensitive personopplysninger er opplysninger som kan avdekke rase eller etnisitet, politiske, religiøse eller filosofiske meninger. Også fagforeningsmedlemskap anses som en sensitiv personopplysning. Videre er helseopplysninger å anse som sensitive personopplysninger. Dette er typisk opplysninger den enkelte tannlege behandler daglig i sitt virke. Som helseopplysninger regnes for eksempel genetiske opplysninger og biometriske data med formål å identifisere en person, samt opplysninger om seksuelle forhold og seksuell orientering. Behandling av sensitive personopplysninger er i utgangspunktet forbudt, med mindre det foreligger lovlig grunnlag for behandlingen.

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, på grunnlag av nasjonal rett eller en avtale med helsepersonell. 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. Se punkt 6 «Vil reglene og normene for tannhelsetjenesten bli endret på grunn av GDPR»

GDPR artikkel 9 nr. 2, ft. 32, 42 og 51.

11. Hva er «behandling» av personopplysninger?

Behandling av personopplysning er enhver aktivitet som er forbundet med en personopplysning, uavhengig av om dette er utført med automatiske midler eller ikke. Kort sagt omfatter «behandling» omtrent all tenkelig bruk og oppbevaring av opplysninger om personer. Eksempler på behandling er innsamling, opptak, lagring, endring, bruk, videresendelse eller på andre måter tilgjengeliggjøring av personopplysninger, også sletting.

Dette omfatter både:

- enhver operasjon (handling) som gjøres med personopplysninger (ved bruk av IT eller ikke), og
- ikke-automatisert behandling (som papir) som inngår eller skal inngå i et register (dvs. strukturerte opplysninger etter særlige kriterier).

GDPR artikkel 2, 4 nr. 2 og 6, ft. 15, 16, 18 og 19

12. Hva er et lovlig behandlingsgrunnlag for personopplysninger?

Det er ikke forbudt å registrere og lagre personopplysninger. I enkelte henseender er det helt nødvendig å innhente og lagre slike opplysninger, f.eks. ved pasientbehandling i en tannlegevirksomhet. Reglene vedrørende personopplysninger skal sørge for at de som behandler slike opplysninger gjør det på en måte som beskytter den enkeltes rett til privatliv.

Lovlig grunnlag for behandling er et av følgende grunnlag:
a) **Samtykke** fra den registrerte, se pasient- og brukerrettighetsloven § 4-1 om informert samtykke

b) Nødvendig for å oppfylle **avtale** som den registrerte er part i eller gjennomføre tiltak på den registrertes anmodning før avtaleinngåelse

c) Oppfylle **rettslig forpliktelse** som påhviler den behandlingsansvarlige

d) Verne den registrertes eller annen persons vitale interesser

e) Utføre en oppgave i allmennhetens interesse eller utøve offentlig myndighet

f) Formål knyttet til berettiget interesse dersom registrertes interesse eller grunnleggende rettigheter går foran/krever vern (**interesseavveining**)

GDPR artikkel 6, ft. 32, 39, 40, 41, 42, 43, 44, 45, 46, 47 og 48.

13. Trenger man en oversikt eller protokoller over behandlingsaktiviteter?

Den behandlingsansvarlige skal føre en behandlingsoversikt og protokoll (register) over behandlingsaktiviteter. Det er imidlertid ikke noe krav å føre slik protokoll om virksomheten har færre enn 250 ansatte. I forbindelse med at man gjør seg klar til GDPR er det anbefalt at det lages en oversikt.

GDPR artikkel 30.

14. Hvem er den registrerte?

Den registrerte er den som personopplysningene omhandler, for eksempel en pasient eller ansatt. Dette vil være en fysisk person som direkte eller indirekte kan identifiseres, særlig ved hjelp av identifikator (som navn, id-nr. eller ett eller flere andre elementer). Merk at juridiske personer (selskaper, organisasjoner mv.) ikke er omfattet av reglene og ikke er å anse som registrerte.

GDPR artikkel 4 nr. 1, ft. 27, 158 og 160

15. Har dette betydning for mine ansatte?

Ja. Forholdet mellom arbeidsgiver og ansatte må reguleres i virksomhetens rutiner for

informasjonssikkerhet og internkontroll.

Se artikkelen «Introduksjon til personvern i arbeidsforhold» som også inkluderer forslag til rutiner for arbeidsgivers innsyn i e-post og sikkerhetsinstruks for ansatte. Se for øvrig «Mal for erklæring om konfidensialitet og sikring av informasjon for ansatte».

16. Har dette betydning for forholdet mellom praksiseiere og assistenttannleger?

Ved samarbeid mellom virksomheter om felles journal, som vil gjelde i de fleste samarbeidsforhold mellom en praksiseier og en assistenttannlege, skal det inngås avtale om felles journal. Dette er allerede regulert i pasientjournalloven § 9.

Se mer om dette i «Samarbeid mellom virksomheter om felles journal –en veileder med avtaleeksempler».

17. Behandlingsansvarlig - hva er det?

Enhver fysisk eller juridisk person, myndighet, organisasjon mv. som:

- bestemmer **formålet** med behandlingen av personopplysninger, og
- bestemmer **hvilke midler** som skal benyttes ved behandlingen
- selv behandler personopplysninger sammen med andre (felles behandlingsansvarlig)

En tannlege er for eksempel behandlingsansvarlig for personopplysninger i et pasientjournalsystem, mens leverandøren av systemet er en databehandler.

GDPR artikkel 4 nr. 7, 24 og 26, ft. 1, 27 og 79.

18. Hva er en databehandler?

En «databehandler» er en fysisk eller juridisk person, offentlig myndighet, institusjon eller ethvert annet organ som behandler personopplysninger på vegne av den behandlingsansvarlige. Dette kan f.eks. være et selskap som leverer et pasientjournalsystem, et lønnssystem og håndterer personopplysninger i denne sammenheng, et dentaldepot eller andre som virksomheten har serviceavtale med, en leverandør med ansvar for en ekstern dataserver osv.

GDPR artikkel 4 nr. 8, 27, 28, ft. 29, 71, 77, 80, 81, 82, 83, 108, 109 og 156.

19. Hvorfor trenger vi ny databehandleravtale?

Det må alltid foreligge en databehandleravtale ved bruk av databehandler. Klinikkeiere må sørge for at for eksempel leverandører av pasientjournalsystemer, lønnssystem o.l. har signert en godkjent databehandleravtale innen 25. mai 2018. Se artikkelen «Hvorfor trenger vi ny databehandleravtale». Vi anbefaler at du bruker vår databehandleravtale.

Avtalen skal blant annet inneholde:

- hensikten med behandlingen
- varigheten av behandlingen
- behandlingens formål og art
- typen personopplysninger og kategorier av registrerte som skal behandles
- den behandlingsansvarliges rettigheter og plikter

Avtalen skal være skriftlig (men kan være elektronisk).

GDPR artikkel 28. ft- 29, 71, 77, 81, 82, 83, 156.

20. Hva er et avvik?

Et avvik er et brudd på personopplysningssikkerheten som fører til ulovlig eller utilsiktet bruk av personopplysninger herunder:

- Tilintetgjøring, tap, endring, ulovlig spredning av eller
- Tilgang til personopplysninger som er overført, lagret eller på andre måter behandlet

Eksempelvis kan en feilsending av en e-post være et avvik dersom e-posten inneholder personopplysninger av et visst omfang, eller sensitive personopplysninger som ikke er krypterte.

Den behandlingsansvarlige skal holde oversikt og dokumentere eventuelle sikkerhetsbrudd. Avvik skal i visse tilfeller meldes til Datatilsynet og de registrerte. Merk at det stilles krav til at avvik registreres/dokumenteres uavhengig av om det aktuelle bruddet skal meldes til Datatilsynet eller ikke. Det anbefales at det lages et internt system for registrering av eventuelle avvik.

GDPR artikkel 4 nr. 12, 33 nr 5 og ft. 73, 85, 86, 87 og 88.

21. Når og hvordan skal det varsles om avvik?

Hovedregelen er at brudd på personopplysningssikkerheten skal varsles. Etter de nye reglene vil den behandlingsansvarlige bli ansvarlig for å varsle Datatilsynet om sikkerhetsbrudd.

Det er imidlertid ikke alle avvik som trenger å meldes til Datatilsynet.

- Det er ikke meldeplikt hvis det er lite trolig at bruddet vil medføre risiko for fysiske personers rettigheter og friheter. Unntaket medfører at det kun er avvik av «et visst omfang» som skal meldes Datatilsynet. Det må med andre ord vurderes om avviket er «av et visst omfang». Slike avvik skal alltid varsles.
- Det er i de fleste tilfeller ikke nødvendig å melde «små avvik» til Datatilsynet. Om bruddet er å anse som lite, må vurderes konkret i hvert tilfelle. Ved «små avvik» kan varsling i de fleste tilfeller unnlates.
- Avvikets alvorlighetsgrad må imidlertid vurderes, dvs. type brudd. Ved alvorlige sikkerhetsbrudd skal det varsles

Frister for melding av avvik:

- Melding om avvik skal sendes fra databehandler til Behandlingsansvarlig uten ugrunnet opphold
- Melding skal sendes fra behandlingsansvarlig til Datatilsynet uten ugrunnet opphold, og senest innen 72 timer fra sikkerhetsbruddet ble oppdaget. Meldes ikke bruddet («av et visst omfang») til Datatilsynet innen 72 timer, skal årsakene til forsinkelsen oppgis.

- Melding skal sendes til de registrerte uten ugrunnet opphold dersom det er høy risiko for rettighetene til registrerte
- Varsling av de registrerte kan unnlates hvis tiltak er innført som reduserer risiko eller ved uforholdsmessig innsats.

Mal for avviksrapport og avvikshåndtering.

Er du i tvil om det skal varsles eller ikke anbefales det å ta kontakt med Datatilsynet for veiledning.

GDPR artikkel 33, ft. 73, 85, 86, 87 og 88.

22. Hva er personvernrådgiver/personvernombud?

De nye reglene om personvernrådgiver/personvernombud er en betydelig utvidelse i forhold til gjeldende norsk rett. Det er imidlertid kun visse typer virksomheter som pålegges å ha rådgiver/ombud, se punkt 23 om «Hvilke virksomheter må ha

personvernrådgiver/personvernombud?».

Det stilles krav til at personvernrådgiver har formalkompetanse (faglige kvalifikasjoner og dybdekunnskap om personvern) og uavhengighet. Oppgavene til en personvernrådgiver vil typisk være å påse at bedriften etterlever reglene om personvern og gi råd til kolleger om de aktuelle reglene. En personvernrådgiver har medbestemmelsesrett vedrørende behandling av personopplysninger, og er bindeledd mot registrerte og offentlige myndigheter.

GDPR artikkel 37 til 39, ft. 97.

23. Hvilke virksomheter må ha personvernrådgiver/personvernombud?

I privat sektor er det bedrifter som har som **hovedvirksomhet** å regelmessig og systematisk monitorere personer, og som behandler **sensitive** personopplysninger eller opplysninger om straffbare forhold i **stor skala** som har plikt til å opprette personvernrådgiver.

Datatilsynet har pr. nå ikke spesifisert hva som ligger i «stor skala» og det må foretas en konkret vurdering i hvert enkelt tilfelle. Datatilsynet har imidlertid uttalt at «vanlige legekontorer» trolig ikke har behov for personvernrådgiver, og derfor vil heller ikke et «vanlig tannlegekontor» ha behov for dette. Unntak vil være dersom det er flere tannleger sammen slik at det behandles særlige kategorier (sensitive) personopplysninger av et større omfang.

Datatilsynet råder alle bedrifter til å dokumentere de vurderinger som er foretatt dersom det ikke opprettes personvernrådgiver, med mindre det er helt opplagt at bedriften ikke er pålagt å ha dette. Dette er særlig viktig hvor flere tannleger arbeider sammen og på den måten er i befatning med et større omfang av sensitive personopplysninger. Vurderingen i den enkelte virksomhet kan f.eks. se slik ut:

«Virksomheten har vurdert at det ikke er pålagt å ha personvernrådgiver etter GDPR artikkel 37, og at det er ikke er nødvendig av andre grunner, siden Virksomheten ikke behandler personopplysninger i stor grad. Det er lagt til grunn at hovedvirksomheten ikke består av behandlingsaktiviteter som på grunn av sin art, omfang og/eller formål krever regelmessig og systematisk monitorering i stor skala av registrerte. Virksomheten behandler ikke i stor skala særlige kategorier (sensitive) personopplysninger foruten pasientopplysninger. Virksomheten er heller ikke offentlig virksomhet som er pålagt å ha personvernrådgiver.»

Se mer om dette i «Trenger min tannlegevirksomhet personvernombud?»

Følgende skal ha personvernrådgiver:

- Kommune, fylkeskommune og stat
- Systematisk overvåkning av registrerte i stor skala
- Virksomheter som i stor skala behandler særlige kategorier personopplysninger / «sensitive personopplysninger» (f.eks. helseopplysninger)

GDPR artikkel 37 til 39, ft. 97.

24. Hvilke krav stilles til sikring av personopplysninger?

Norsk helsenett er utviklet med tanke på sikker behandling av helseopplysninger. Den behandlingsansvarlige og databehandler skal for øvrig gjennomføre egnede tekniske og organisatoriske tiltak for å sikre og påvise at behandlingen gjennomføres etter forordningen, hensyntatt behandlingens:

- Art
- Omfang

- Formål
- Sammenhengen den utføres i
- Risikoene av varierende sannsynlighets- og alvorlighetsgrad
- Skal lages retningslinjer for vern av personopplysninger
- Må overholde godkjente adferdsnormer og sertifiseringsmekanismer

Se mer om dette under punkt 6 «Vil reglene og bransjenormene for tannhelsetjenesten bli endret på grunn av GDPR?» og punkt 7 «Hva gjør jeg med de andre personopplysningene i virksomheten? Risikovurdering og rutiner for informasjonssikkerhet og internkontroll»

GDPR artikkel 24 og 28, ft. 29, 71, 74, 77, 81-83

25. Er det en informasjonsplikt overfor de registrerte?

Ja, de registrerte skal blant annet informeres om:
- Identiteten og kontaktopplysninger til behandlingsansvarlig (samt representant og personvernrådgiver)
- Formålene med behandlingen
- Rettslig grunnlag for behandlingen
- Eventuelle mottakere eller kategorier av mottakere av personopplysninger
- Eventuell overføring av personopplysninger til en tredjestat mv.
- Tidsrommet opplysningene vil bli lagret
- Retten til innsyn, korrigering og sletting eller begrensning av behandling. Vær oppmerksom på at det er særregler for redigering, retting og sletting av pasientjournal, i helsepersonelloven §§ 42-44, jf. journalforskriften § 13.
- Retten til å klage til Datatilsynet
- Kategorier av personopplysninger

Informasjonsplikten kan vanligvis oppfylles gjennom personvernerklæringen, se punkt 26 «Hva er personvernerklæring, og trenger jeg det?»

GDPR artikkel 12, 13 og 14, ft. 39, 50, 53, 58, 57, 59, 60, 64, 66, 68, 75, 85 og 164.

26. Hva er personvernerklæring, og trenger jeg det?

Alle bedrifter må ha en personvernerklæring, som f.eks. kan henges opp på venteværelset og legges ut på virksomhetens hjemmeside. Se «Personvernerklæring til nettsider og venteværelset».

En personvernerklæring skal fortelle hvordan den enkelte bedrift samler inn og bruker personopplysninger. En slik erklæring skal blant annet inneholde opplysninger om:

- Hvem som er behandlingsansvarlig
- Hva som er formålet med behandlingen av personopplysningene
- Hva som er det rettslige grunnlaget for behandlingen (hjemmel)
- Hvilke personopplysninger som behandles
- Hvor opplysningene hentes fra
- Er det frivillig å gi fra seg opplysningene?
- Utleveres opplysningene til tredjeparter?
- Hvilke rutiner har bedriften for sletting og arkivering av personopplysninger?
- Opplysninger om den registrertes rettigheter
- Kontaktinformasjon for innsyn, retting eller sletting

27. Har den registrerte rett til innsyn?

Retten til innsyn gjelder kun for den registrerte.

1. Den registrerte har rett til besvarelse av om opplysninger behandles

2. Den registrerte har rett til informasjon om behandlingen, herunder:
- Formålet med behandlingen
- (Kategorier) mottakere som opplysninger er eller skal utleveres til
- Hvor lenge opplysningene forventes lagret eller kriteriene for å fastsette denne perioden
- Retten til å kreve korrigering eller sletting eller begrensning av/protestering mot behandling
- Retten til å klage til Datatilsynet
- Hvor personopplysningene kommer fra
- Om det vil skje automatiserte avgjørelser, herunder profilering, og logikken og betydningen for behandlingen for den registrerte

3. Den registrerte har rett til utlevering av alle opplysninger
- Må kun gis til den registrerte (sikre at det er rett mottaker)
- Må ikke utlevere personopplysninger om andre ved innsynet. Det skal besvares elektronisk dersom henvendelsen kommer elektronisk. Hevendelsen må besvares innen en måned (kan utsettes til 2 måneder). I utgangspunktet kostnadsfritt for den registrerte. Det er et unntak fra innsyn: Anmodningen om innsyn er åpenbart grunnløs eller overdreven (som ved gjentakelse).

Det er særregler for innsyn i og utlevering av pasientjournal, i bl.a. pasient- og brukerrettighetsloven § 5-1, jf. journalforskriften § 12.

GDPR artikkel 12 og 15, ft. 39, 57, 58, 59, 60 og 64.

28. Hva er dataportabilitet? Overføring av personopplysninger

Dataportabilitet betyr at den registrerte kan kreve å få sine personopplysninger overført fra en virksomhet til en annen. Formålet er å gi den registrerte kontroll over sine egne opplysninger. Retten til dataportabilitet gjelder imidlertid kun egne opplysninger som den registrerte selv har gitt til den behandlingsansvarlige.

Dataportabilitet kan skje ved at den registrerte får utlevert personopplysninger i et strukturert, alminnelig anvendt og maskinlesbart format slik at disse kan overføres til en annen behandlingsansvarlig. I den grad det er teknisk mulig har den registrerte rett til å få personopplysningene overført direkte fra en behandlingsansvarlig til en annen.

Ved overføring av personopplysninger til andre, herunder andre behandlingsansvarlige (som for eksempel ved henvisning eller kommunikasjon med tekniker) og tredjeparter, skal det undersøkes om mottaker har lovlig behandlingsgrunnlag. Personopplysninger skal ikke overføres dersom mottakeren ikke har behandlingsgrunnlag eller om dette er uklart, eller om det er usikkert om mottakeren kan behandle personopplysningene på lovlig og sikker måte.

Overføring av personopplysningene skal skje på sikker måte, som sikrer personopplysningenes konfidensialitet og integritet.

Det er kun Norsk helsenett som er godkjent for elektronisk overføring av helseopplysninger per i dag. Alternativet er ordinær postforsendelse. Det er flere særregler for pasientopplysninger, bl.a. pasientjournalloven § 24 om overføring av pasientjournal.

GDPR artikkel 20.

29. Hva er retten til å bli glemt?

Den registrerte får ved GDPR en tydeligere rett til å kreve sletting av egne personopplysninger. Retten til å kreve sletting kalles retten til å bli glemt. Den registrerte kan blant annet kreve at opplysningene om han/henne slettes når opplysningene ikke lenger er nødvendig for å oppnå formålet med behandlingen, samtykket til behandlingen er trukket tilbake og det ikke finnes et annet rettslig grunnlag for behandlingen, den registrerte har fremsatt en berettiget innsigelse og hvor personopplysninger er blitt behandlet på en måte som ikke er lovlig. Retten til å bli glemt - «sletteplikten» - gjelder imidlertid ikke dersom opplysningene er nødvendig for at den behandlingsansvarlige skal kunne oppfylle en rettslig forpliktelse, den er nødvendig for allmenhetens interesse knyttet til folkehelse og videre når den er nødvendig for arkivformål i allmennhetens interesse.

Det er særregler for oppbevaring og sletting av helseopplysninger, bl.a. i pasientjournalloven § 25, helsepersonelloven §§ 42 og 43 og journalforskriften §§ 13 og 14

GDRP artikkel 17.

30. Hva skjer om en bryter GDPR reglene?

Datatilsynet har ansvaret for å føre tilsyn med at reglene etterleves i Norge. Datatilsynet kan ilegge overtredelsesgebyr dersom de finner at noen bryter reglene. Ved utmålingen av overtredelsesgebyret skal det legges vekt på overtredelsens alvor, graden av skyld, om overtredelsen kunne vært forebygget, om det foreligger gjentagelse etc. GDPR åpner for at Datatilsynet kan ilegge et overtredelsesgebyr på opptil 20 millioner euro eller hvis det gjelder foretak, 4 % av den globale årsomsetningen i forutgående regnskapsår hvis denne er høyere. Disse rammene vil være aktuelle for grove overtredelser hos større bedrifter.